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

For Calendar Years 2015, 2016, and 2017

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

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

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

Introduction

Section 13424(a) of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), requires the Secretary of the Department of Health and Human Services (the Department) to prepare and submit an annual report[1] to the Senate Committee on Health, Education, Labor, and Pensions and to the House Committee on Ways and Means and the House Committee on Energy and Commerce (the Committees), regarding compliance with the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191), as well as the privacy, security, and breach notification provisions of the HITECH Act. Thus, for the years for which the report is prepared, the report summarizes the Department's compliance and enforcement activities with respect to the HIPAA Privacy, Security, and Breach Notification Rules at 45 CFR Parts 160 and 164 (collectively, the HIPAA Rules or the Rules). Section 13424(a)(2) of the HITECH Act requires that each report be made available to the public on the website of the Department. This report is available at http://www.hhs.gov/ocr/privacy.

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

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

This report is prepared for calendar years 2015, 2016, and 2017. 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.

[1] This Report covers a three-year period.

Background

HIPAA was enacted on August 21, 1996. Subtitle F of HIPAA, known as the Administrative Simplification provisions permitted the Secretary to establish standards for the privacy and security of individually identifiable health information held by an entity subject to HIPAA, defined in the HIPAA Rules as a "covered entity." Briefly, 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 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 or as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

The HIPAA Security Rule, found at 45 CFR Part 160 and Subparts A and C of Part 164, establishes national standards to protect electronic PHI created, received, used or maintained by covered entities and their business associates. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI (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, and information about the Department's efforts to enforce the Rules during calendar years 2015, 2016, and 2017.

---

[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 http://www.hhs.gov/ocr/privacy, describes the types and numbers of breaches reported to the Secretary and the actions that have been taken by covered entities and business associates in response to the reported breaches.

Enforcement Process

OCR enforces the HIPAA Rules by investigating written complaints filed with OCR, either on paper, by e-mail, or through its complaint portal. OCR also conducts compliance reviews of circumstances brought to its attention, to determine if covered entities or business associates are in compliance with the Rules. In addition, OCR's compliance activities include conducting audits[4] and providing education and outreach to foster compliance with the Rules' requirements, 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 taken place after compliance with the Rules was required. OCR cannot investigate complaints regarding actions that took place before compliance with the HIPAA Rules was required.

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

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

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

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

[4] Section 13411 of the HITECH Act, which became effective on February 17, 2010, authorizes and 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 is wrapping up and the permanent audit program will be implemented thereafter.

Compliance Reviews

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

Investigations

Once OCR initiates an investigation, OCR collects evidence, through interviews, witness statements, requests for data from the entity involved, information from 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 the covered entity or business associate did not violate the requirements of 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 requirements of the HIPAA Rules. In such cases, OCR will generally first attempt to resolve the case with the covered entity or business associate 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 the covered entity or business associate undertook the required corrective action to resolve the allegations. In the vast majority of cases, a covered entity or business associate will, through voluntary cooperation and corrective action, be able to demonstrate satisfactory compliance with the HIPAA Rules.

Resolution Agreements

Where OCR finds indications of noncompliance due to willful neglect, or where the nature and scope of the noncompliance warrants additional enforcement action, OCR pursues a resolution agreement with a payment of a settlement amount and an obligation to complete a corrective action plan. In these cases, OCR notifies the covered entity or business associate that, while OCR is prepared to assess a CMP with regard to the alleged violations of the HIPAA Rules, OCR is willing to negotiate the terms of a resolution agreement and corrective action plan to resolve the indications of noncompliance. These settlement agreements have involved the payment of a monetary amount that is some fraction of the potential CMPs for which the covered entity or business associate would be liable in the case. Additionally, in most cases, the resolution agreement includes a corrective action plan that requires the covered entity or business associate to fix remaining compliance issues; in many cases, the corrective action plan requires

the covered entity or business associate to undergo monitoring of its compliance with the HIPAA Rules for a specified period of time. While this type of resolution still constitutes informal action on the part of OCR, resolution agreements and corrective action plans are powerful enforcement tools for OCR.

Civil Money Penalties

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

From the 2003 compliance date of the HIPAA Privacy Rule through the end of calendar year 2017, out of all the cases OCR attempted to resolve informally through a resolution agreement, three cases have resulted in the imposition of a CMP.[5]

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 Rules, 2) ensure covered entities and business associates are adequately safeguarding PHI, and 3) ensure individuals are provided the rights afforded to them by the Rules.

Through the use of funds available under the HITECH Act, OCR engaged the services of a professional public accounting firm to conduct the pilot audit program in 2011-2012. As part of this pilot, OCR established a comprehensive audit protocol containing the HIPAA regulatory requirements to be assessed in the audits.

Throughout 2013, OCR analyzed the findings of the pilot audits to uncover trends, potential best practices, and vulnerabilities. In addition, OCR engaged PriceWaterhouse Coopers (PWC) to conduct an evaluation of the pilot audit program. The evaluation included surveys of audited entities, review of the protocols, and examination of the audit program structure and documentation. OCR received the final report from PWC in November 2013.

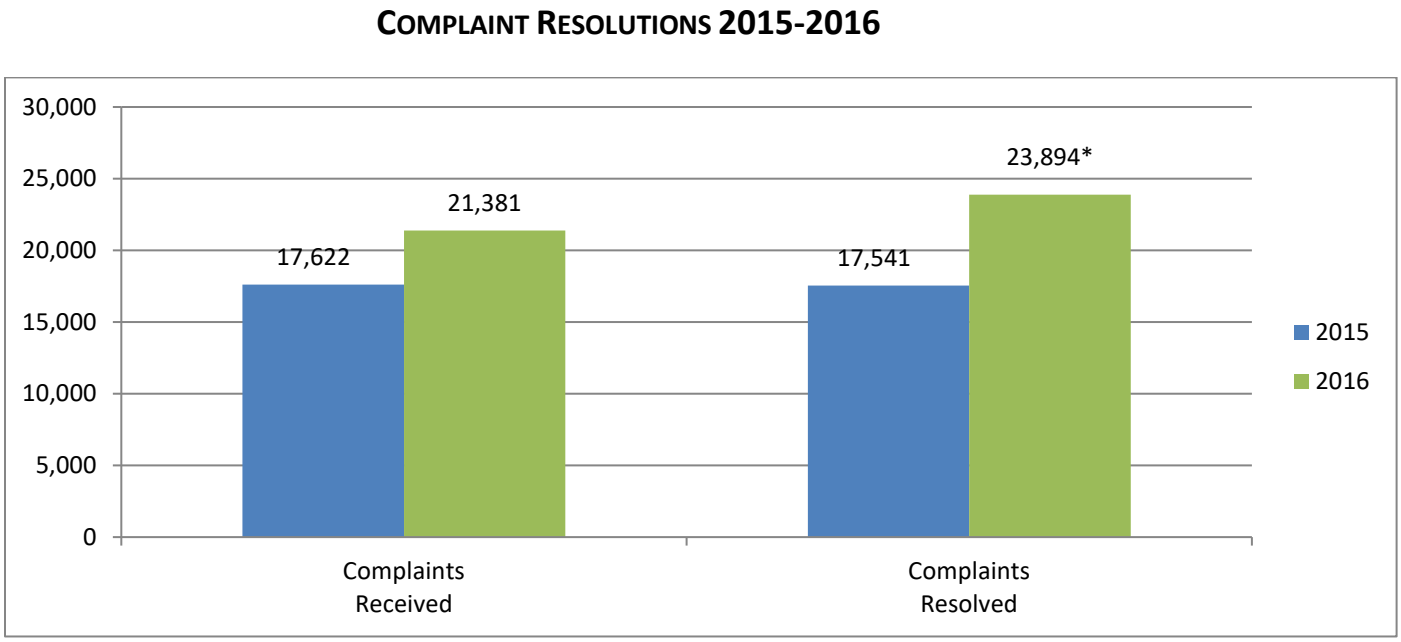
[5] All resolution agreements entered into by the Department prior to February 17, 2010, contained settlement amounts that were paid to the General Treasury. Pursuant to the HITECH Act, after February 17, 2010, settlement amounts or CMPs are paid to, and used by, OCR for enhanced enforcement of the HIPAA Rules.

In 2014, OCR began preparing for the second phase of the audit program. Planning activities included revising the entity screening questionnaire intended to gather data about the size, complexity, and operations of potential auditees. This data assisted in objectively selecting audit subjects that to the extent possible, represented a broad cross section of entities covered by HIPAA. OCR also updated the audit protocol to reflect the new regulatory requirements implemented through the January 25, 2013 Omnibus final rule to assure Phase 2 of the program would include audits of both covered entities and business associates. OCR developed an online portal for entity document submission and a module within its Program Information Management System to administer and manage the audit program. The new module allowed for more efficient workflows; electronic work papers; draft findings reports; and final reports. Other activities in 2014 and 2015 included development of additional guidance responsive to issues found through the pilot audits.

Enforcement Data

Complaint Resolutions

2015 and 2016 Complaints



*More complaints were resolved than received because OCR resolves complaints from prior years.

Figure 1

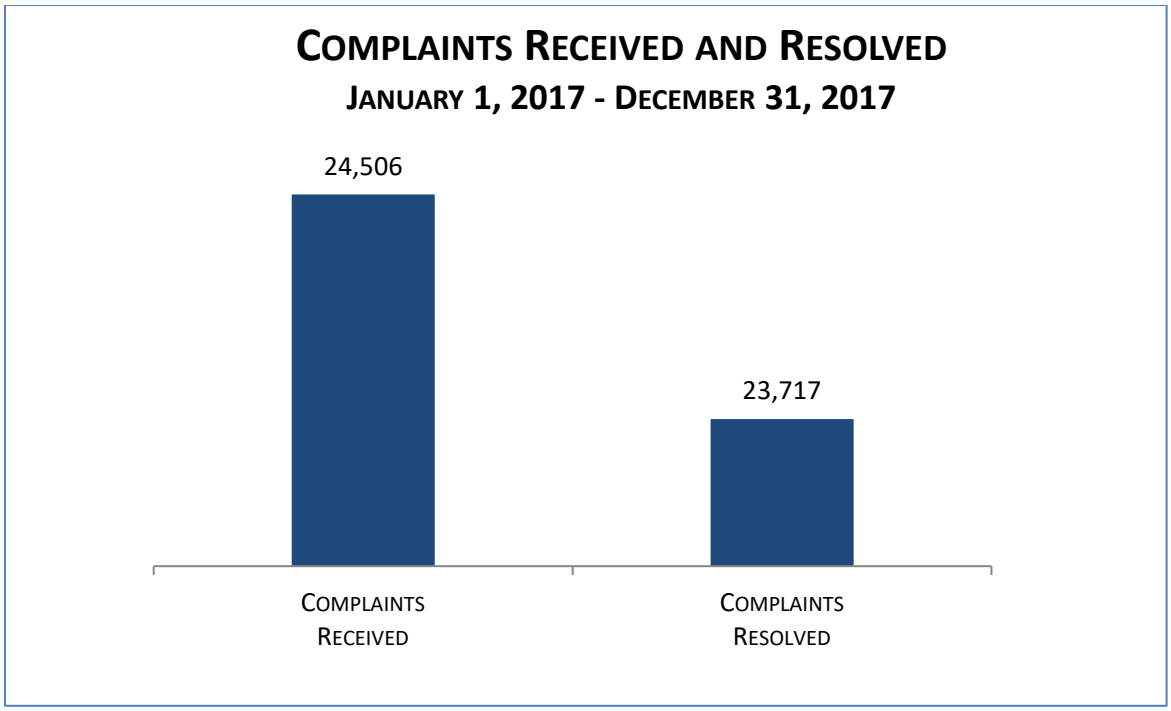


Figure 2

2015 Complaints

During calendar year 2015, OCR received 17,622 new complaints and carried over 5,739 complaints from 2014. OCR resolved a total of 17,541 (75%) complaints in 2015. One complaint was resolved through monetary settlement totaling $218,400. No complaints were resolved through imposition of civil money penalties.

In 12,634 cases (72% of complaints resolved), OCR determined that the complaint did not present an eligible case for enforcement of the HIPAA Rules. In these cases, OCR lacked jurisdiction under the HIPAA Rules because the complaint alleged a violation prior to the compliance date of the applicable Rule, alleged a violation by an entity not covered by the HIPAA Rules, was untimely or withdrawn, described an activity that did not violate the HIPAA Rules, or alleged an activity that OCR could not independently substantiate. In 3,817 cases (22% of the complaints resolved) in 2015, OCR provided pre-investigational technical assistance to the covered entity or business associate. In 730 cases (4% of the total complaints resolved; 67% of the investigated complaints), OCR provided post-investigational technical assistance, or required the covered entity or business associate to take corrective action. In 360 cases (2% of the total complaints resolved; 33% of the investigated complaints), OCR found that no violation of the HIPAA Rules had occurred. See Figure 3.

2015 Complaint Resolutions

January 1, 2015 through December 31, 2015

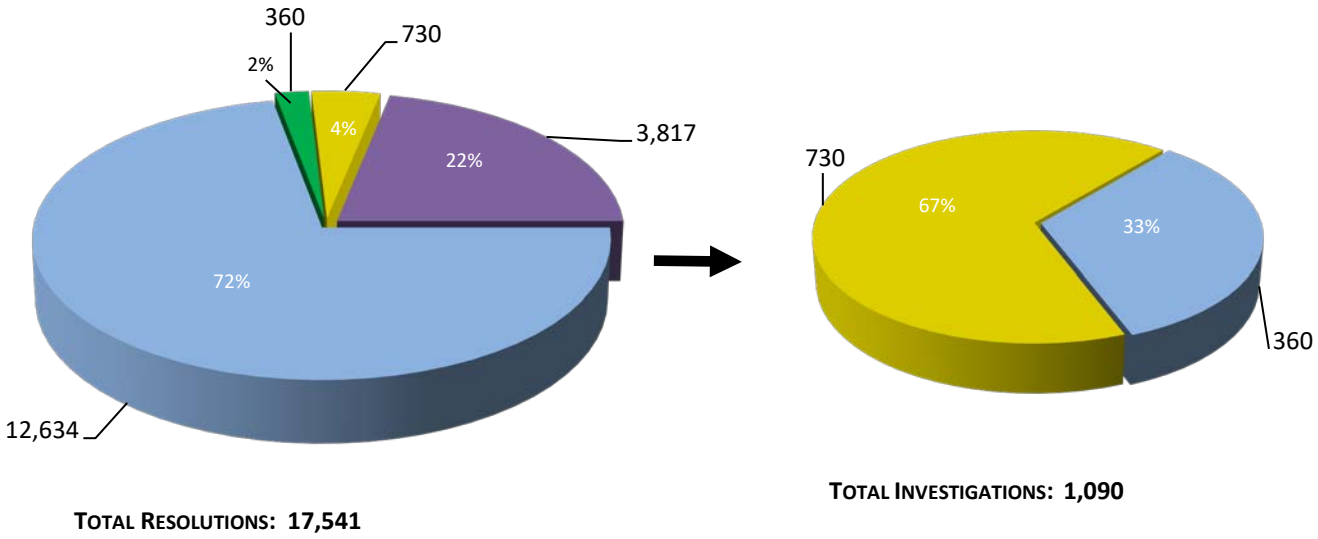


Figure 3

For the 17,640 complaints OCR received in 2015, the top five issues were Impermissible Uses and Disclosures, Safeguards, Administrative Safeguards (Security Rule), Access, and Technical Safeguards (Security Rule). These issues accounted for approximately 11 percent of resolved complaints.

2016 Complaints

During calendar year 2016, OCR received 21,381 new complaints and carried over approximately 5,481 from the previous year. OCR resolved a total of 23,894 complaints. One complaint was resolved through monetary settlement totaling $25,000 and one through imposition of $239,800 in CMPs.

In 16,780 cases (70%), OCR determined the complaint alleged a violation prior to the compliance date of the applicable Rule, alleged a violation by an entity not covered by the HIPAA Rules, was untimely or withdrawn, described an activity that did not violate the HIPAA Rules, or alleged an activity that OCR could not independently substantiate. In 6,204 cases (26%) in 2016, OCR provided pre-investigational technical assistance to the covered entity or business associate. In 706 cases (3% of the total complaints resolved; 67% of the complaints investigated), after investigation OCR provided technical assistance to the covered entity or business associate or required the covered entity or business associate to take corrective action.

Finally, in 204 cases (1% of the total complaints resolved; 33% of the complaints investigated), OCR found that no violation of the HIPAA Rules had occurred. See Figure 4.

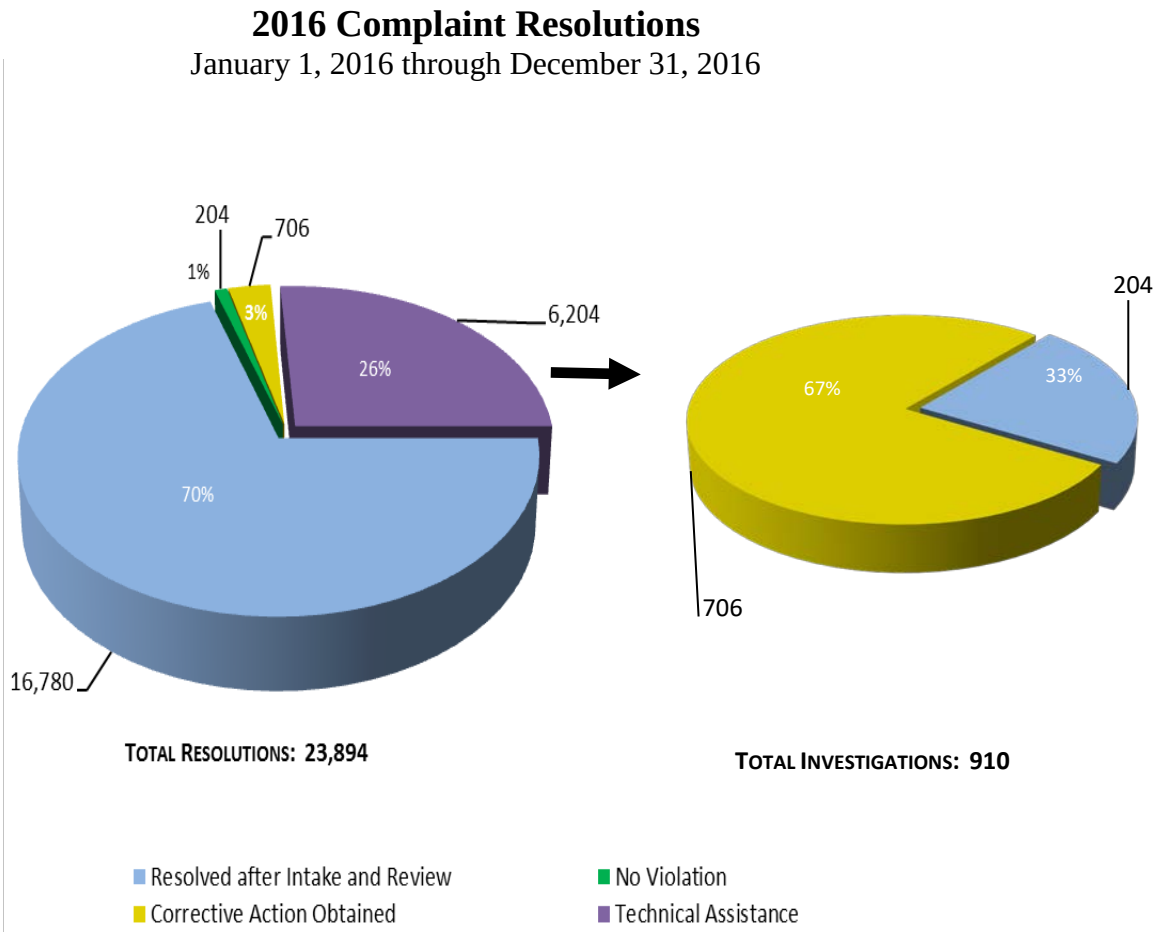


Figure 4

For the 21,381 complaints OCR received in 2016, the top five issues were Access, Impermissible Uses and Disclosures, Safeguards, Administrative Safeguards (Security Rule), and Technical Safeguards (Security Rule). These issues accounted for approximately six percent of resolved complaints.

OCR received 3,741 more complaints in 2016 as compared to 2015, an increase of 21 percent. (17,640 cases received in 2015 compared to 21,381 cases in 2016).

2017 Complaints

During calendar year 2017, OCR received 24,506 new complaints and carried over approximately 3,115 cases from the previous year. OCR resolved a total of 23,717 complaints.

In 2017, OCR resolved 15,269 cases (64%) before initiating an investigation by determining that the complaint either (1) alleged a violation prior to the compliance date of the applicable Rule, (2) alleged a violation by an entity not covered by the HIPAA Rules, (3) was untimely or withdrawn, (4) described an activity that did not violate the HIPAA Rules, and/or (5) alleged an activity that OCR could not independently substantiate. OCR resolved 7,307 cases (31%) by providing technical assistance before initiating an investigation.

OCR investigated 1141 cases. For 669 of these cases, OCR required the covered entity or business associate to take corrective action (3% of the total complaints resolved, 59% of the complaints investigated), for 219 of these cases, OCR provided technical assistance after investigation (1% of the total complaints resolved, 19% of the complaints investigated). In 253 cases investigated (1% of the total complaints resolved, 22% of the complaints investigated), OCR found that no violation of the HIPAA Rules had occurred. See Figure 5.

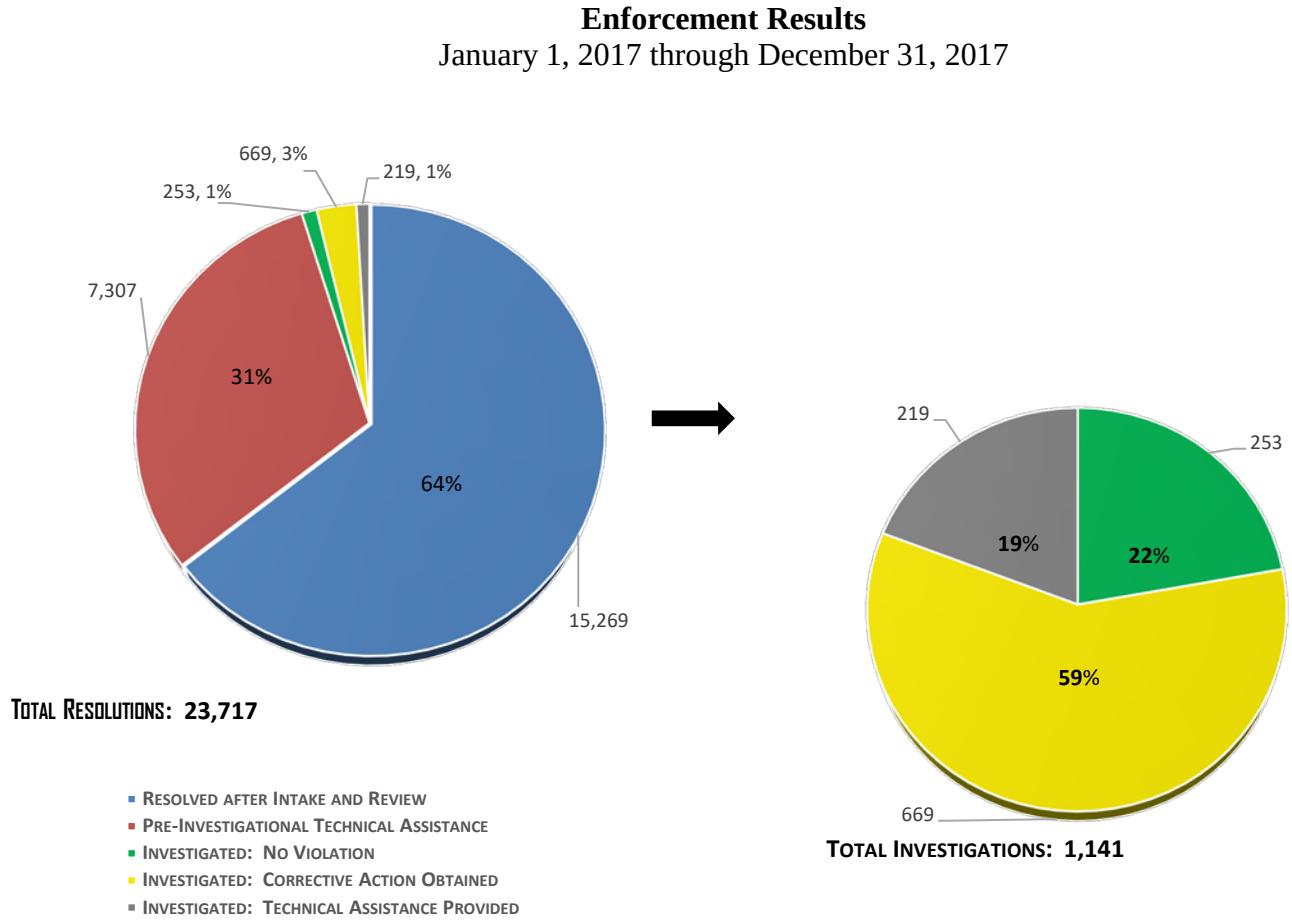


Figure 5

Of the 24,506 complaints OCR received, one complaint was resolved through monetary settlement totaling $387,200. No complaints were resolved by assessing civil money penalties.[6]

For the 23,717 complaints OCR resolved in 2017, the top five issues were Impermissible Uses and Disclosures, Safeguards, Administrative Safeguards (Security Rule), Access, and Technical Safeguards (Security Rule). These issues accounted for approximately ten percent of resolved complaints.

OCR received 3,102 more complaints in 2017 as compared to 2016, an increase of 14 percent (21,404 cases received in 2016 compared to 24,506 cases received in 2017).

Compliance Reviews

Compliance reviews are initiated from a breach report filing, an incident brought to the attention of OCR based on media reports, referrals from other federal agencies, or as a result of patterns observed over a series of complaints. A separate report to Congress, available at http://www.hhs.gov/ocr/privacy, 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 reported breaches.

2015 Compliance Reviews

During calendar year 2015, OCR opened 322 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 269 reviews were opened as a result of breach reports affecting 500 or more individuals.[7] The remaining 53 compliance reviews were opened based on an event or incident brought to OCR's attention through other avenues as stated above.

OCR closed 184 compliance reviews in 2015. Of these closed cases, 148 originated from breach reports and 36 originated from other means. After an investigation in 150 cases (82%), the covered entity or business associate took corrective action. OCR found that no violation of the HIPAA Rules had occurred in 16 cases (9%). OCR closed the breach compliance review without requiring corrective actions or making recommendations in eight cases (4%), for example, because the case was referred to another federal agency, or OCR determined that the complaint alleged an activity that could not be independently substantiated. OCR determined that it did not have jurisdiction under the HIPAA Rules to investigate the allegations in ten cases (5%) because the complaint alleged a violation prior to the compliance date of the applicable Rule, alleged a violation by an entity not covered by the HIPAA Rules, was untimely or withdrawn, or described an activity that did not violate the HIPAA Rules. See Figure 6.

[6] OCR resolved one breach investigation by imposing civil money penalties for $3.2 million. The nature of the case is more fully described in the summary of Children's Medical Center of Dallas found in the Appendix.
[7] 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.

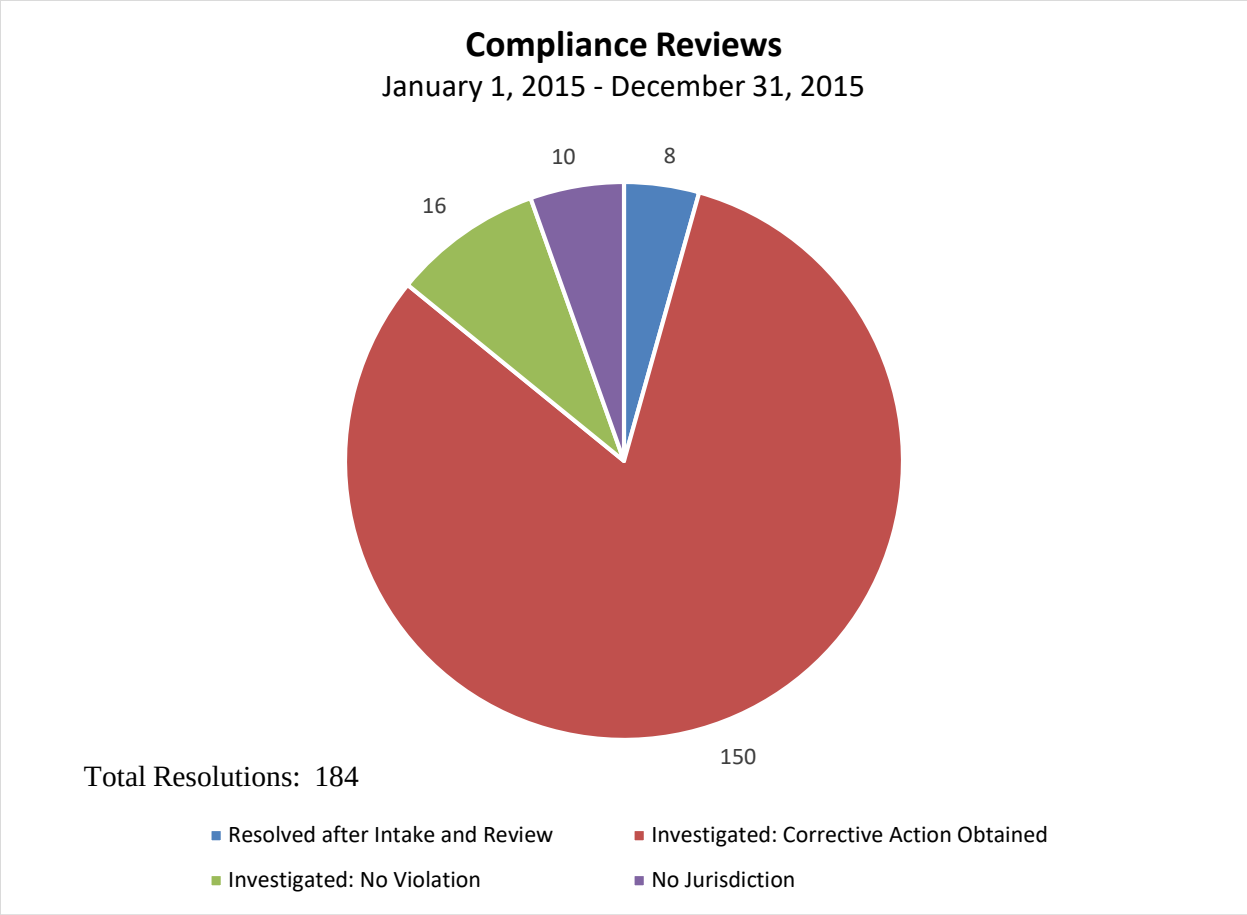


Figure 6

2016 Compliance Reviews

During calendar year 2016, OCR opened 384 compliance reviews to investigate potential violations of the HIPAA Rules. Of these, 327 compliance reviews were opened as a result of a breach report affecting 500 or more individuals.[8] The remaining 57 compliance reviews were initiated by OCR based on media reports, referrals from other federal agencies, or through patterns seen through a series of complaints.

OCR closed 334 compliance reviews in 2016. Of the closed cases, 319 originated from breach reports and 15 originated from other means. After an investigation in 293 cases (88%), the covered entity or business associate took corrective action. OCR found that no violation of the HIPAA Rules had occurred in 28 cases (8%). OCR closed breach compliance reviews without requiring corrective actions or making recommendations in four cases (1%). OCR determined that it did not have jurisdiction to investigate the allegations in nine cases (3%) because the complaint alleged a violation prior to the compliance date of the applicable Rule, alleged a violation by an entity not covered by the HIPAA Rules, was untimely or withdrawn, or described an activity that did not violate the HIPAA Rules. See Figure 7.

[8] *Id.*

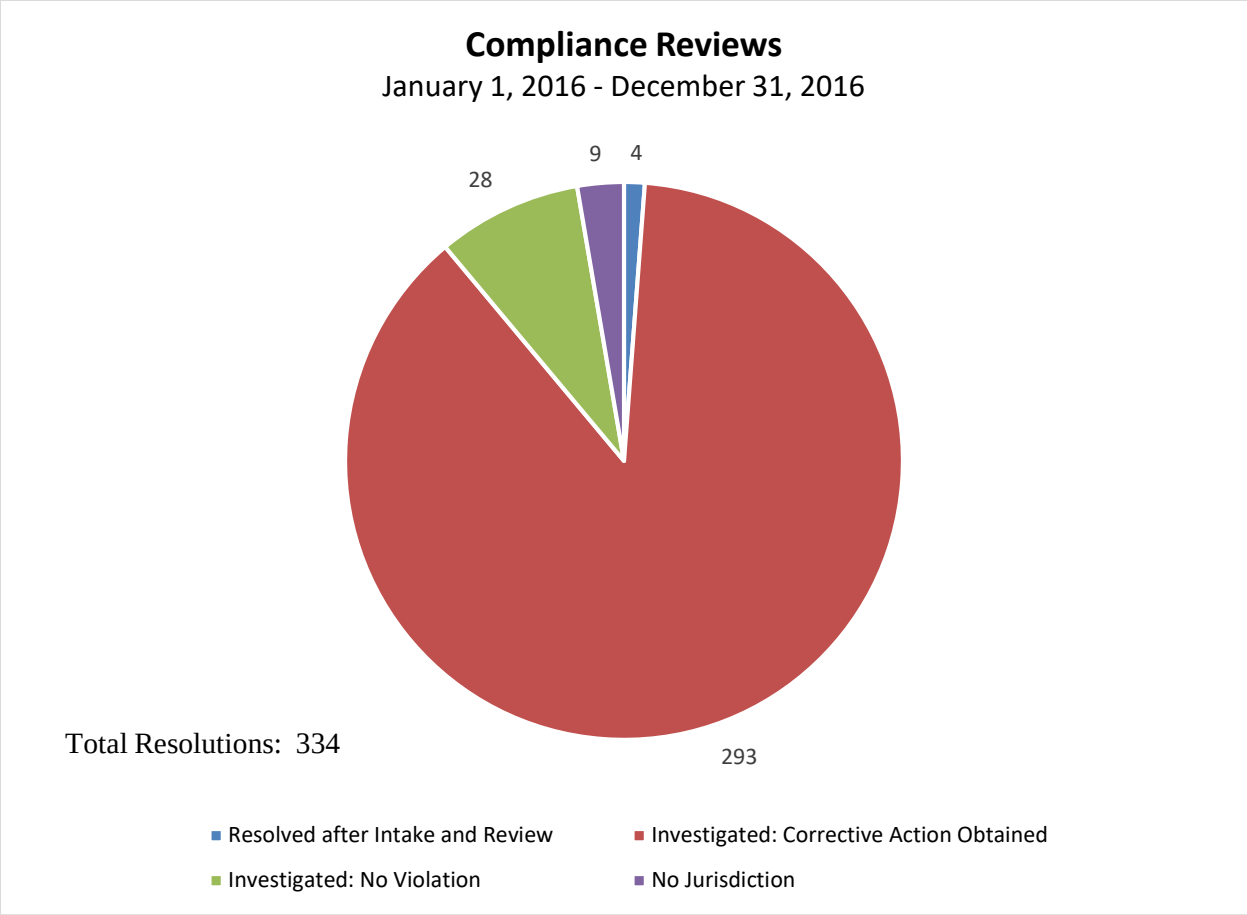


Figure 7

2017 Compliance Reviews

During calendar year 2017, OCR opened 469 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 359 compliance reviews were a result of a breach report affecting 500 or more individuals.[9] The remaining 110 compliance reviews were opened based on an event or incident brought to OCR's attention through other mechanisms.

OCR closed 396 compliance reviews in 2017. Of the closed cases, 371 originated from breach reports and 25 originated from other means. The covered entity or business associate took corrective action or paid a civil money penalty in 345 cases (87%). OCR found that no violation of the HIPAA Rules had occurred in 29 cases (7%). OCR closed breach compliance reviews without requiring corrective actions or making recommendations in 13 cases (3%). OCR determined that it did not have jurisdiction under the HIPAA Rules to investigate the allegations in nine cases (2%) because the complaint alleged a violation prior to the compliance date of the applicable Rule, alleged a violation by an entity not covered by the HIPAA Rules, was untimely or withdrawn, or described an activity that did not violate the HIPAA Rules. See Figure 8.

[9] *Id.*

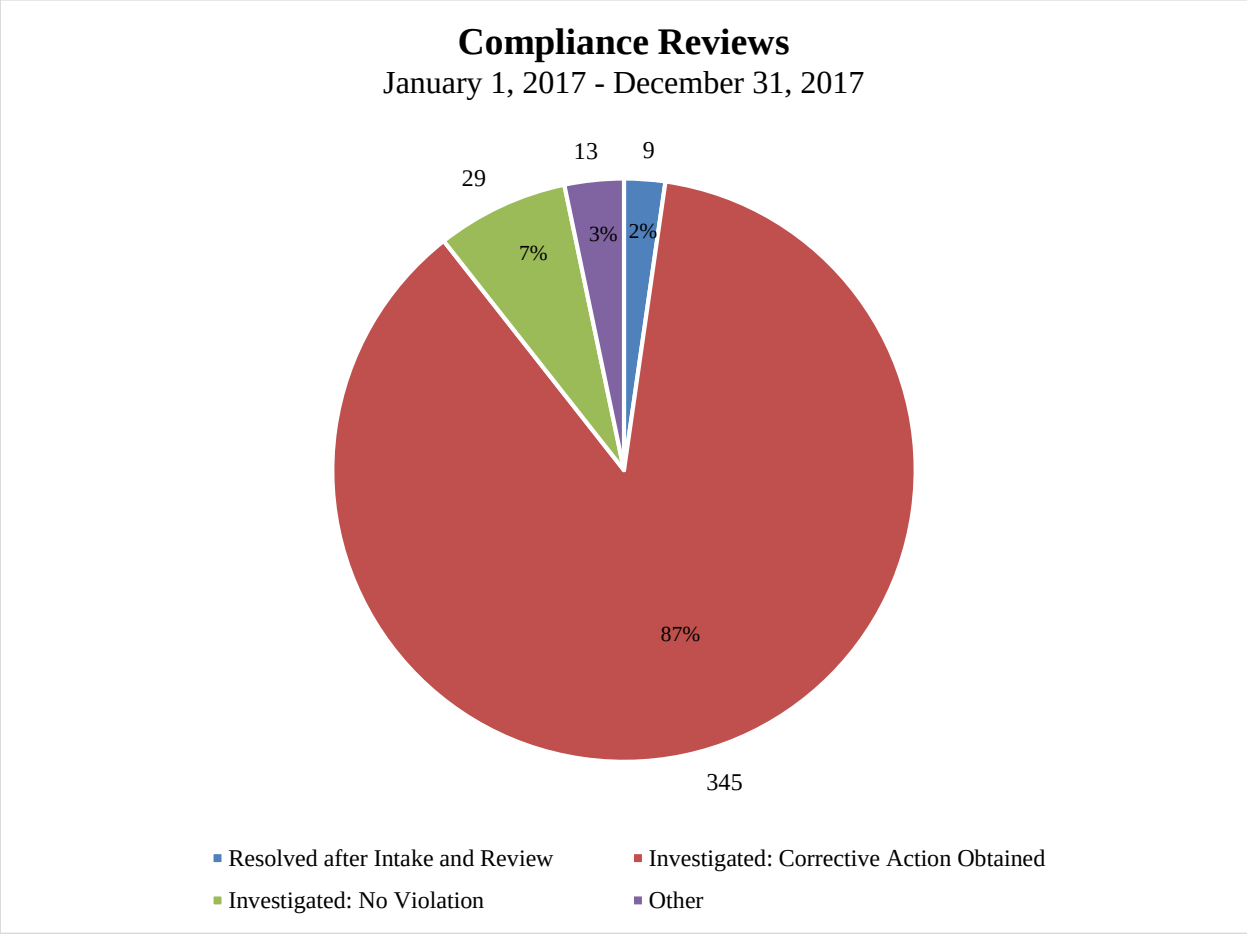


Figure 8

Subpoenas

OCR did not issue any subpoenas in 2015 or 2016. OCR issued three subpoenas in 2017.

Audits

In 2015, OCR engaged Federal Consulting, Inc., to augment its staff and conduct a host of planning activities for the second phase of the audit program. OCR launched Phase 2 of the audit program in 2016. In this phase, OCR reviewed policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security and Breach Notification Rules.

The 2016 audit process began with verification of an entity's address and contact information. An email was sent to covered entities and business associates requesting that contact information be provided to OCR in a timely manner. OCR then transmitted a pre-audit questionnaire that was used to gather data about the size, type, and operations of potential auditees; this data was used,

with other information, to create potential audit subject pools. If an entity did not respond to these requests for information, OCR used the information that was otherwise available about the organization to move forward with its audit program. Failure to respond did not shield an organization from being selected for an audit or from becoming the subject of a compliance review. OCR communicated via email and encouraged entities to check their spam filtering and virus protection services to ensure email notifications were not incorrectly classified as spam.

Using a random sampling methodology, OCR selected over 200 entities as subjects of the HIPAA compliance desk audits. Selected covered entities received audit notification letters along with requests to provide specific documentation to demonstrate their compliance with selected privacy, security and breach notification provisions. Additionally, covered entities were asked to provide a list of their business associates. OCR used these listings to create the business associate selection pool. Auditors reviewed documentation provided by each covered entity and business associate to develop draft findings that OCR then shared with the entity. Auditees were given ten business days to respond to these draft findings. Their written responses were included in the final audit report. Audit reports generally describe how the audit was conducted, include any findings, and attach entity responses to the draft findings.

Using the audit protocol and more specific test procedures, OCR assessed entity efforts of complying with a select set of provisions. Desk audits targeted particular provisions that were the source of a significant compliance failures in the pilot audits, as well compliance reviews and compliant investigations.

Covered entity desk audits examined:

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

Business associate desk audits examined:

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

OCR's audits will enhance industry awareness of compliance obligations, and enable OCR to better target technical assistance to identified problems. Through the information gleaned from the audits, OCR will develop tools and guidance to assist the industry in compliance self-evaluation, and in preventing breaches. OCR will evaluate the results and procedures used in Phase 2 audits to develop the permanent HIPAA compliance audit program.

OCR completed desk audits and its examination of documentation for 166 covered entities in September 2017 and 41 business associates in December 2017. These audits found that all types of audited entities fail to implement effective risk analysis and risk management strategies pursuant to the HIPAA Security Rule, and most audited entities fail to adequately safeguard protected health information and ensure individual access as required by the HIPAA Privacy Rule. Additionally, some covered entities omitted required statements from their notices of privacy practices. Aggregate findings from Phase 2 of the audit program will be published in 2019.

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

OCR continued to build its public outreach and education efforts in support of the HITECH Act's mandate to increase education to both HIPAA covered entities and consumers, and to address compliance deficiencies in the regulated community that have been identified by complaint investigations, compliance reviews, and the audit program. In 2015, 2016, and 2017, OCR worked to develop materials in plain language that help consumers better understand their rights under HIPAA and to provide the regulated community with technical assistance and best practices that promote better compliance with the HIPAA Rules. OCR's 2015, 2016, and 2017 outreach efforts include:

- OCR launched a redesigned, plain language website, featuring audience segmentation that allows consumers and professionals to more easily find information on the HIPAA Privacy, Security and Breach Notification Rules. The website redesign underwent an extensive user experience review that helped inform efforts to improve overall site navigation and to enhance customer satisfaction by improving usability. The redesigned site features a responsive, mobile-first design and enhanced search engine optimization. The new site was launched in December 2015, and content is updated regularly to ensure that information is fresh and relevant. According to Google Analytics and ForeSee data, OCR's HIPAA pages receive over 250,000 unique visits a month.

- In 2015, 2016, and 2017, OCR co-hosted its annual "Safeguarding Health Information: Building Assurance through HIPAA Security" conference with the National Institute for Standards and Technology. The two-day annual conference explored the current health information technology security landscape, and offers practical strategies, tips and techniques for complying with the HIPAA Security Rule. Attendees chose to participate on-site or through a live webcast. The two-day annual conference explored the current health information technology security landscape, and offers practical strategies, tips and techniques for complying with the HIPAA Security Rule. Attendees choose to participate on-site or through a live webcast.

- In collaboration with the Office of the National Coordinator for Health Information Technology (ONC), OCR helped create "Your Health Information, Your Rights!" -- a series of three short, educational videos (in English with an option for Spanish captions) to help individuals understand their right under HIPAA to access and receive a copy of their health information. As part of this effort, OCR and ONC also created a one-page

fact sheet, with illustrations, that provides a summary of individuals' rights under HIPAA.

- In February 2016, OCR launched a series of periodic cybersecurity newsletters to better inform the regulated community of the various security threats and vulnerabilities that currently exist in the healthcare sector, to understand what security measures can be taken to decrease the possibility of being exposed by these threats, and how to reduce breaches of ePHI. OCR published 11 newsletters on a variety of topics to provide best practices and other practical information to help HIPAA covered entities and business associates practice better cyber hygiene.

- OCR launched the second phase of its "Information is Powerful Medicine" campaign to help raise awareness about the right to access health information under HIPAA, and to empower individuals to better participate in their own medical care. In addition to print materials, the campaign website at http://www.hhs.gov/getitcheckituseit provides links to factsheets, videos, and key messages to enable individuals to better understand how HIPAA gives you the right to see and get copies of your health information. Having access to your medical information can mean better communication between you and your doctors, less paperwork and greater control over your health. Efforts continue to disseminate print materials and to drive traffic to the campaign website through digital ads and other health promotion strategies.

- OCR launched on-line provider education training, enabling health care professionals to obtain free continuing medical education and continuing educations credits, on key aspects of, and their legal responsibilities under HIPAA and how the individual's right to obtain their health information assists individuals to become more involved in their own care. OCR trained a total of 24,756 clinician learners, with 4,686 CME/CE credits issued in 2017. Because of this success rate, OCR has renewed this activity for Fiscal Year 2019, beginning in October 2018.

Appendix

Significant Activities: Resolution Agreements, CMPs, and Subpoenas[10] in 2015, 2016, and 2017

Resolution Agreement with Cornell Prescription Pharmacy

Cornell Prescription Pharmacy (Cornell) agreed to settle potential violations of the Privacy Rule with OCR. Cornell paid $125,000 and agreed to adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. Cornell is a small, single-location pharmacy that provides in-store and prescription services to patients in the Denver, Colorado metropolitan area, specializing in compounded medications and services for hospice care agencies in the area.

OCR opened a compliance review and investigation after receiving notification from a local Denver news outlet regarding the disposal of unsecured documents containing the PHI of 1,610 patients in an unlocked, open container on Cornell's premises. The documents were not shredded and contained identifiable information regarding specific patients. Evidence obtained by OCR during its investigation revealed Cornell's failure to implement any written policies and procedures as required by the HIPAA Privacy Rule. Cornell also failed to provide training on policies and procedures to its workforce as required by the Privacy Rule.

In addition to the $125,000 settlement amount, the agreement requires Cornell to:

- Develop and implement a comprehensive set of policies and procedures to comply with the HIPAA Privacy Rule; and
- Train its workforce members on these HIPAA policies and procedures.

This settlement occurred in April of 2015.

Resolution Agreement with St. Elizabeth's Medical Center

St. Elizabeth's Medical Center (SEMC) agreed to settle potential violations of the HIPAA Privacy, Security and Breach Notification Rules with OCR. SEMC paid $218,400 and agreed to adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. SEMC is a tertiary care hospital located in Brighton, Massachusetts that offers both inpatient and outpatient services.

On November 16, 2012, OCR received a complaint alleging noncompliance with the HIPAA Rules by SEMC workforce members. Specifically, the complaint alleged that workforce members impermissibly used an internet-based document sharing application to store documents containing the ePHI of at least 498 individuals. SEMC also failed to timely identify and respond to a known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome. Additionally, on August 25, 2014, SEMC submitted

[10] Information provided here on Resolution Agreements, CMPs, and Subpoenas is based on the year in which the Agreement was signed, the CMP assessed, or the Subpoena issued. In most instances, investigations of these cases were initiated in years prior to 2015, 2016, or 2017.

notification to OCR regarding a breach of unsecured ePHI stored on a former SEMC workforce member's personal laptop and USB flash drive, which affected 595 individuals. OCR's investigations indicated that SEMC disclosed the PHI of at least 1,093 individuals, and failed to implement sufficient security measures regarding the transmission and storage of ePHI to reduce risks and vulnerabilities to a reasonable and appropriate level.

In addition to the $218,400 settlement amount, the agreement requires SEMC to:

- Complete a self-assessment on its workforce members familiarity and compliance with the transmission of ePHI using unauthorized networks, storing ePHI on unauthorized information systems, including unsecured networks and devices, removal of ePHI from the medical center, prohibition on sharing accounts and passwords for access or storage, encryption of portable devices that access or store ePHI, and security incident reporting related to ePHI;
- Review and revise its workforce training pursuant to self-assessment; and
- Review and revise its policies pursuant to self-assessment.

This settlement occurred in July of 2015.

Resolution Agreement with Cancer Care Group

Cancer Care Group (Cancer Care) agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. Cancer Care paid $750,000 and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Cancer Care Group is a radiation oncology private physician practice, with 13 radiation oncologists serving hospitals and clinics throughout Indiana.

On August 29, 2012, OCR received notification from Cancer Care regarding a breach of unsecured ePHI after a laptop bag was stolen from an employee's car. The bag contained the employee's computer and unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information, and clinical information of approximately 55,000 current and former Cancer Care patients.

OCR's subsequent investigation found that, prior to the breach, Cancer Care was in widespread non-compliance with the HIPAA Security Rule. It had not conducted an enterprise-wide risk analysis before the breach occurred in July 2012. Further, Cancer Care did not have in place a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, even though this was common practice within the organization. OCR found that these two issues, in particular, contributed to the breach, as an enterprise-wide risk analysis could have identified the removal of unencrypted backup media as an area of significant risk to Cancer Care's ePHI, and a comprehensive device and media control policy could have provided employees with direction in regard to their responsibilities when removing devices containing ePHI from the facility.

In addition to the $750,000 settlement, the resolution agreement requires Cancer Care to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an organization-wide risk management plan;
- Review and revise HIPAA Security Rule policies and procedures; and
- Review and revise HIPAA Security Rule training program.

This settlement occurred in August of 2015.

Resolution Agreement with Lahey Hospital and Medical Center

Lahey Hospital and Medical Center (Lahey) agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. Lahey paid $850,000 and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Lahey is a non-profit teaching hospital affiliated with Tufts Medical School, providing primary and specialty care in Burlington, Massachusetts.

Lahey notified OCR that a laptop was stolen from an unlocked treatment room during the overnight hours on August 11, 2011. The laptop was on a stand that accompanied a portable CT scanner; the laptop operated the scanner and produced images for viewing through Lahey's Radiology Information System and Picture Archiving and Communication System. The laptop hard drive contained the PHI of 599 individuals. Evidence obtained through OCR's subsequent investigation indicated widespread non-compliance with the HIPAA rules, including:

- Failure to conduct a thorough risk analysis of all of its ePHI;
- Failure to physically safeguard a workstation that accessed ePHI;
- Failure to implement and maintain policies and procedures regarding the safeguarding of ePHI maintained on workstations utilized in connection with diagnostic/laboratory equipment;
- Lack of a unique user name for identifying and tracking user identity with respect to the workstation at issue in this incident;
- Failure to implement procedures that recorded and examined activity in the workstation at issue in this incident; and
- Impermissible disclosure of 599 individuals' PHI.

In addition to the $850,000 settlement, Lahey agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an organization-wide risk management plan; and
- Develop or revise as necessary written policies and procedures for device and media controls, workstation security, and audit controls.

This settlement occurred in November of 2015.

Resolution Agreement with Triple-S Management Corporation

Triple-S Management Corporation ("TRIPLE-S"), on behalf of its wholly owned subsidiaries, Triple-S Salud Inc., Triple-C Inc. and Triple-S Advantage Inc., formerly known as American

Health Medicare Inc., agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. TRIPLE-S paid $3.5 million and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program, an effort it had already begun at the time of settlement.

TRIPLE-S is an insurance holding company based in San Juan, Puerto Rico, which offers a wide range of insurance products and services to residents of Puerto Rico through its subsidiaries. TRIPLE-S cooperated with HHS in investigating this case and agreed to put in place a comprehensive HIPAA compliance program as a condition for settlement.

After receiving multiple breach notifications from TRIPLE-S involving unsecured PHI, OCR initiated investigations to ascertain the entities' compliance with HIPAA Rules. OCR's investigations indicated widespread non-compliance throughout the various subsidiaries of Triple-S, including:

- Failure to implement appropriate administrative, physical, and technical safeguards to protect the privacy of its beneficiaries' PHI;
- Impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement;
- Use or disclosure of more PHI than was necessary to carry out mailings;
- Failure to conduct an accurate and thorough risk analysis that incorporates all IT equipment, applications, and data systems utilizing ePHI; and
- Failure to implement security measures sufficient to reduce the risks and vulnerabilities to its ePHI to a reasonable and appropriate level.

In addition to the $3.5 million settlement, TRIPLE-S agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an organization-wide risk management plan;
- Evaluate any environmental or operation changes that affect the security of ePHI;
- Review and revise as necessary HIPAA Privacy and Security Rule policies and procedures; and
- Train workforce members on revised HIPAA Privacy and Security Rule policies and procedures.

This settlement occurred in November of 2015.

<u>Resolution Agreement with University of Washington Medicine</u>

The University of Washington Medicine (UWM) agreed to settle charges that it potentially violated the HIPAA Security Rule by failing to implement policies and procedures to prevent, detect, contain, and correct security violations. UWM is an affiliated covered entity, which includes designated health care components and other entities under the control of the University of Washington, including University of Washington Medical Center, the primary teaching hospital of the University of Washington School of Medicine. Affiliated covered entities must have in place appropriate policies and processes to assure HIPAA compliance with respect to each of the entities that are part of the affiliated group. The settlement includes a monetary

payment of $750,000, a corrective action plan, and annual reports on the organization's compliance efforts.

OCR initiated its investigation of the UWM following receipt of a breach report on November 27, 2013, which indicated that the ePHI of approximately 90,000 individuals was accessed after an employee downloaded an email attachment that contained malicious malware. The malware compromised the organization's IT system, affecting the data of two different groups of patients: (1) approximately 76,000 patients involving a combination of patient names, medical record numbers, dates of service, and/or charges or bill balances; and (2) approximately 15,000 patients involving names, medical record numbers, other demographics such as address and phone number, dates of birth, charges or bill balances, Social Security numbers, insurance identification or Medicare numbers.

OCR's investigation indicated UWM's security policies required its affiliated entities to have up-to-date, documented system-level risk assessments and to implement safeguards in compliance with the Security Rule. However, UWM did not ensure that all of its affiliated entities were properly conducting risk assessments and appropriately responding to the potential risks and vulnerabilities in their respective environments.

In addition to the $750,000 settlement, UWM agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities; and
- Develop an organization-wide risk management plan.

This settlement occurred in December of 2015.

Civil Money Penalty involving Lincare

An HHS Administrative Law Judge (ALJ) ruled that Lincare, Inc. (Lincare) violated the HIPAA Privacy Rule and granted summary judgment to OCR on all issues, requiring Lincare to pay $239,800 in CMPs imposed by OCR. This is only the second time in its history that OCR sought a CMP for HIPAA violations and both times the penalties have been upheld by the administrative law judge.

Lincare is a provider of respiratory care, infusion therapy, and medical equipment to in-home patients, with more than 850 branch locations in 48 states. OCR's investigation of Lincare began after an individual complained that a Lincare employee left behind documents containing the PHI of 278 patients after moving residences. Evidence established that this employee removed patients' information from the company's office, left the information exposed in places where an unauthorized person had access, and then abandoned the information altogether. Over the course of the investigation, OCR found that Lincare had inadequate policies and procedures in place to safeguard patient information that was taken offsite, although employees, who provide health care services in patients' homes, regularly removed material from the business premises. Further evidence indicated that the organization had an unwritten policy requiring certain employees to store protected health information in their own vehicles for extended periods of time. Although

aware of the complaint and OCR's investigation, Lincare subsequently took only minimal action to correct its policies and strengthen safeguards to ensure compliance with the HIPAA Rules.

Lincare claimed that it had not violated HIPAA because the PHI was "stolen" by the individual who discovered it on the premises previously shared with the Lincare employee. The ALJ rejected this argument, in agreement with OCR: "[U]nder HIPAA, Respondent [Lincare] was obligated to take reasonable steps to protect its PHI from theft."

This decision awarding the CMP occurred in January of 2016.

Resolution Agreement with Complete P.T., Pool & Land Physical Therapy, Inc.

Complete P.T., Pool & Land Physical Therapy, Inc. (Complete P.T.) agreed to settle violations of the HIPAA Privacy and Security Rules with OCR. Complete P.T. is a physical therapy practice located in the Los Angeles area. Complete P.T. paid $25,000, agreed to the adoption and implementation of a corrective action plan, and annual reporting of compliance efforts for a one year period.

On August 8, 2012, OCR received a complaint alleging that Complete P.T. had impermissibly disclosed numerous individuals' PHI, when it posted patient testimonials, including full names and full face photographic images, to its website without obtaining valid, HIPAA-compliant authorizations. OCR's investigation revealed that Complete P.T.:

- Failed to reasonably safeguard PHI;
- Impermissibly disclosed PHI without an authorization; and
- Failed to implement policies and procedures with respect to PHI that were designed to comply with HIPAA's requirements with regard to authorization.

In addition to the $25,000 settlement, Complete P.T. agreed to:

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

This settlement occurred in February of 2016.

Resolution Agreement with North Memorial Health Care

North Memorial Health Care of Minnesota (North Memorial) paid $1.55 million to settle charges that it potentially violated the HIPAA Privacy and Security Rules by failing to enter into a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information. North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities.

OCR initiated its investigation of North Memorial following receipt of a breach report on September 27, 2011, which indicated that an unencrypted, password-protected laptop was stolen from a business associate's workforce member's locked vehicle, impacting the ePHI of 9,497 individuals.

OCR's investigation indicated that North Memorial failed to have in place a business associate agreement, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and health care operations activities on its behalf. North Memorial gave its business associate, Accretive Health, Inc., access to North Memorial's hospital database, which stored the ePHI of 289,904 patients. Accretive also received access to non-electronic protected health information as it performed services on-site at North Memorial.

The investigation further determined that North Memorial failed to complete a risk analysis to address all of the potential risks and vulnerabilities to the ePHI that it maintained, accessed, or transmitted across its entire IT infrastructure -- including but not limited to all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes.

In addition to the $1.55 million settlement, North Memorial agreed to:

- Develop an organization-wide risk analysis and risk management plan; and
- Train appropriate workforce members on all policies and procedures newly developed or revised pursuant to its corrective action plan.

This settlement occurred in March of 2016.

Resolution Agreement with Feinstein Institute for Medical Research

Feinstein Institute for Medical Research (Feinstein) paid OCR $3.9 million to settle potential violations of the HIPAA Privacy and Security Rules and agreed to undertake a substantial corrective action plan to bring its operations into compliance. Feinstein is a biomedical research institute that is organized as a New York not-for-profit corporation and is sponsored by Northwell Health, Inc., formerly known as North Shore Long Island Jewish Health System, a large health system headquartered in Manhasset, New York that is comprised of twenty one hospitals and over 450 patient facilities and physician practices.

OCR's investigation began after Feinstein filed a breach report indicating that, on September 2, 2012, a laptop computer containing the ePHI of approximately 13,000 patients and research participants was stolen from an employee's car. The ePHI stored in the laptop included the names of research participants, dates of birth, addresses, social security numbers, diagnoses, laboratory results, medications, and medical information relating to potential participation in a research study.

OCR's investigation discovered that Feinstein's security management process was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity. Further, Feinstein lacked policies and procedures for authorizing access to ePHI by its workforce members, failed to

implement safeguards to restrict access to unauthorized users, and lacked policies and procedures to govern the receipt and removal of laptops that contained ePHI into and out of its facilities. For electronic equipment procured outside of Feinstein's standard acquisition process, Feinstein failed to implement proper mechanisms for safeguarding ePHI as required by the Security Rule.

In addition to the $3.9 million settlement, Feinstein agreed to:

- Develop an organization-wide risk analysis and risk management plan;
- Evaluate any environmental or operation changes that affect the security of ePHI; and
- Review and revise, if necessary, HIPAA Privacy and Security policies and procedures.

This settlement was formalized in March of 2016.

Resolution Agreement with Raleigh Orthopaedic

Raleigh Orthopaedic Clinic, P.A. of North Carolina (Raleigh Orthopaedic) paid $750,000 to settle charges that it potentially violated the HIPAA Privacy Rule by handing over PHI for approximately 17,300 patients to a potential business partner without first executing a business associate agreement. HIPAA covered entities cannot disclose PHI to unauthorized persons, and the lack of a business associate agreement left this sensitive health information without safeguards and vulnerable to misuse or improper disclosure. Raleigh Orthopaedic is a provider group practice that operates clinics and an orthopaedic surgery center in the Raleigh, North Carolina area.

OCR initiated its investigation of Raleigh Orthopaedic following receipt of a breach report on April 30, 2013. OCR's investigation indicated that Raleigh Orthopaedic released the x-ray films and related protected health information of 17,300 patients to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. Raleigh Orthopedic failed to execute a business associate agreement with this entity prior to turning over the x-rays (and PHI).

In addition to the $750,000 payment, Raleigh Orthopaedic is required to:

- Revise its policies and procedures;
- Establish a process for assessing whether entities are business associates;
- Designate a responsible individual to ensure business associate agreements are in place prior to disclosing PHI to a business associate;
- Create a standard template business associate agreement;
- Establish a standard process for maintaining documentation of a business associate agreements for at least six (6) years beyond the date of termination of a business associate relationship; and
- Limit disclosures of PHI to any business associate to the minimum necessary to accomplish the purpose for which the business associate was hired.

This settlement occurred in April of 2016.

Resolution Agreement with New York Presbyterian Hospital

OCR reached a $2.2 million settlement with New York Presbyterian Hospital (NYP) for the egregious disclosure of two patients' PHI to film crews and staff during the filming of "NY Med," an ABC television series, without first obtaining authorization from the patients. In particular, OCR found that NYP allowed the ABC crew to film someone who was dying and another person in significant distress, even after a medical professional urged the crew to stop.

By allowing individuals receiving urgent medical care to be filmed without their authorization by members of the media, NYP's actions blatantly violate the HIPAA Rules, which were specifically designed to prohibit the disclosure of individual's PHI, including images, in circumstances such as these.

OCR also found evidence that NYP failed to safeguard PHI and allowed ABC film crews virtually unfettered access to its health care facility, effectively creating an environment where PHI could not be protected from impermissible disclosure to the ABC film crew and staff. In addition to the $2.2 million, OCR will monitor NYP for two years as part of this settlement agreement, helping ensure that NYP will remain compliant with its HIPAA obligations while it continues to provide care for patients.

In addition to the $2.2 million settlement, NYP agreed to:

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

This settlement occurred in April of 2016.

Resolution Agreement with Catholic Health Care Services of the Archdiocese of Pennsylvania

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) agreed to settle potential violations of the HIPAA Security Rule after the theft of a CHCS mobile device compromised the PHI of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement included a monetary payment of $650,000 and a corrective action plan.

OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee iPhone. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan.

In determining the resolution amount, OCR considered that CHCS provides unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS.

OCR will monitor CHCS for two years as part of this settlement agreement, helping ensure that CHCS will remain compliant with its HIPAA obligations while it continues to act as a business associate.

In addition to the $650,000 settlement, CHCS agreed to:

- Develop an organization-wide risk analysis and risk management plan;
- Develop, maintain, review and revise, if necessary, Security Policies and Procedures; and
- Provide documentation of all business associate agreements where CHCS acts as a business associate to a covered entity; and
- Train workforce members on HIPAA Security Rule policies and procedures.

This settlement occurred in June of 2016.

Resolution Agreement with Oregon Health and Science University

Oregon Health & Science University (OHSU) agreed to settle potential violations of HIPAA Privacy and Security Rules following an investigation by OCR that found widespread and diverse problems at OHSU, which will be addressed through a comprehensive three-year corrective action plan. The settlement includes a monetary payment by OHSU to the Department for $2.7 million.

OCR's investigation began after OHSU submitted multiple breach reports affecting thousands of individuals, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive. These incidents each garnered significant local and national press coverage. OCR's investigation uncovered evidence of widespread vulnerabilities within OHSU's HIPAA compliance program, including the storage of the ePHI of over 3,000 individuals on a cloud-based server without a business associate agreement. OCR found significant risk of harm to 1,361 of these individuals due to the sensitive nature of their diagnoses. The server stored a variety of ePHI including credit card and payment information, diagnoses, procedures, photos, driver's license numbers and Social Security numbers.

OHSU performed risk analyses in 2003, 2005, 2006, 2008, 2010, and 2013, but OCR's investigation found that these analyses did not cover all ePHI in OHSU's enterprise, as required by the Security Rule. While the analyses identified vulnerabilities and risks to ePHI located in many areas of the organization, OHSU did not act in a timely manner to implement measures to address these documented risks and vulnerabilities. OHSU also lacked policies and procedures to prevent, detect, contain, and correct security violations and failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for ePHI maintained on its workstations, despite having identified this lack of encryption as a risk.

OHSU is a large public academic health center and research university centered in Portland, Oregon, comprising two hospitals, and multiple general and specialty clinics throughout Portland and throughout the State of Oregon.

In addition to the $2.7 million settlement agreement, OHSU agreed to:

- Develop an organization-wide risk analysis and risk management plan;
- Provide update on encryption status including a mobile device management solution and status for laptops, desktops and medical equipment; and
- Provide security awareness training to workforce members.

This settlement occurred in July of 2016.

Resolution Agreement with University of Mississippi Medical Center

The University of Mississippi (UM) Medical Center (UMMC) agreed to settle multiple alleged violations of HIPAA with OCR. During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach. UMMC paid $2.75 million and agreed to adopt a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

On March 21, 2013, OCR was notified of a breach, after UMMC's privacy officer discovered that a password-protected laptop was missing from UMMC's Medical Intensive Care Unit (MICU). UMMC's investigation concluded that it had likely been stolen by a visitor to the MICU who had inquired about borrowing one of the laptops. OCR's investigation revealed that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via UMMC's wireless network, because users could access an active directory containing 67,000 files after entering a generic username and password. The directory included 328 files containing the ePHI of an estimated 10,000 patients dating back to 2008.

Further, OCR's investigation revealed that UMMC:

- Failed to implement appropriate policies and procedures to prevent, detect, contain, and correct security violations;
- Failed to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users;
- Failed to assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI; and
- Failed to notify each individual whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach.

UM is Mississippi's sole public academic health science center, with education and research functions in addition to providing patient care in four specialized hospitals on the Jackson campus and at clinics throughout Jackson and the State. Its designated health care component,

UMMC, includes University Hospital, the site of the breach in this case, located on the main UMMC campus in Jackson.

In addition to the $2.75 million settlement, UMMC agreed to:

- Designate an internal monitor to review UMMC's compliance with corrective action plan;
- Develop an organization-wide risk analysis and risk management plan;
- Update Security Rule policies and procedures;
- Revise Breach Notification Policies;
- Develop plan to implement unique user identification; and
- Provide security awareness training to workforce members.

This settlement occurred in July of 2016.

Resolution Agreement with Advocate Health Care Network

Advocate Health Care Network (Advocate) agreed to a settlement with OCR, for multiple potential violations of HIPAA involving ePHI. Advocate paid $5.55 million and agreed to adopt a corrective action plan. This significant settlement, the largest to-date involving a single entity, is a result of the extent and duration of the alleged noncompliance (dating back to the inception of the Security Rule in some instances), the involvement of the Illinois State Attorney General in a corresponding investigation, and the large number of individuals whose information was affected by Advocate, one of the largest health systems in the country.

OCR began its investigation in 2013, when Advocate submitted three breach notification reports pertaining to separate and distinct incidents involving its subsidiary, Advocate Medical Group ("AMG"). The combined breaches affected the ePHI of approximately 4 million individuals. The ePHI included demographic information, clinical information, health insurance information, patient names, addresses, credit card numbers and their expiration dates, and dates of birth. OCR's investigations into these incidents revealed that Advocate:

- Failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its ePHI;
- Failed to implement policies and procedures and facility access controls to limit physical access to the electronic information systems housed within a large data support center;
- Failed to obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession; and
- Failed to reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

Advocate Health Care Network is the largest fully-integrated health care system in Illinois, with more than 250 treatment locations, including ten acute-care hospitals and two integrated children's hospitals. Its subsidiary, AMG, is a non-profit physician-led medical group that provides primary care, medical imaging, outpatient and specialty services throughout the Chicago area and in Bloomington-Normal, Illinois.

In addition to the $5.55 million settlement, Advocate agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an enterprise-wide risk management plan;
- Evaluate any environmental or operation changes that affect the security of ePHI;
- Develop an encryption report regarding status of all devices and equipment that may used to access, store, download or transmit ePHI;
- Review and revise policies and procedures on device and media controls; facility access controls; and business associates; and
- Develop enhanced Privacy and Security Awareness Training.

This settlement occurred in August of 2016.

Resolution Agreement with Care New England Health System (Women and Infants Hospital)

Care New England Health System (CNE), on behalf of each of the covered entities under its common ownership or control, agreed to settle potential violations of HIPAA Privacy and Security Rules. The settlement included a monetary payment of $400,000 and a comprehensive corrective action plan. CNE provides centralized corporate support for its subsidiary affiliated covered entities, which include a number of hospitals and health care providers in Massachusetts and Rhode Island. These functions include, but are not limited to, finance, human resources, information services and technical support, insurance, compliance and administrative functions.

On November 5, 2012, OCR received notification from Woman & Infants Hospital of Rhode Island (WIH), a covered entity member of CNE, of the loss of unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals, including patient name, dates of birth, dates of exams, physicians' names, and, in some instances Social Security Numbers. As WIH's business associate, CNE provides centralized corporate support including technical support and information security for WIH's information systems. WIH provided OCR with a business associate agreement with Care New England Health System effective March 15, 2005, that was not updated until August 28, 2015, as a result of OCR's investigation, and therefore, did not incorporate revisions required under the HIPAA Omnibus Final Rule.

OCR's investigation found the following:

- From September 23, 2014 until August 28, 2015, WIH disclosed PHI and allowed its business associate, CNE, to create, receive, maintain, or transmit PHI on its behalf, without obtaining satisfactory assurances as required under HIPAA. WIH failed to renew or modify its existing written business associate agreement with CNE to include the applicable implementation specifications required by the HIPAA Privacy and Security Rules.
- From September 23, 2014, until August 28, 2015, WIH impermissibly disclosed the PHI of at least 14,004 individuals to its business associate when WIH provided CNE with access to PHI without obtaining satisfactory assurances, in the form of a written business associate agreement, that CNE would appropriately safeguard the PHI.

With respect to the underlying breach, on July 17, 2014, WIH entered into a consent judgment with the Massachusetts Attorney General's Office (AGO), and reached a settlement of $150,000. OCR found the consent judgment to sufficiently cover most of the conduct in this breach, including the failure to implement appropriate safeguards related to the handling of the PHI contained on the backup tapes and the failure to provide timely notification to the affected individuals. While the AGO's actions do not legally preclude OCR from imposing a CMP, OCR determined not to include additional potential violations in this case for the purposes of settlement, given that such potential violations had already been addressed by the AGO and based on OCR's policy approach to concurrent cases with State AGOs.

In addition to the $400,000 settlement, CNE agreed to:

- Review and revise, if necessary, HIPAA Privacy and Security Policies and Procedures; and
- Train workforce members on HIPAA Privacy and Security Rule policies and procedures

This settlement occurred in September of 2016.

Resolution Agreement with St. Joseph Health Ministry

St. Joseph Health Ministry (SJH) agreed to settle potential violations of HIPAA Privacy and Security Rules, following the report that files containing ePHI were publicly accessible through internet search engines from 2011 until 2012. SJH, a non-profit integrated Catholic health care delivery system sponsored by the St. Joseph Health Ministry, paid a settlement amount of $2.14 million and agreed to adopt a comprehensive corrective action plan. SJH's range of services includes 14 acute care hospitals, home health agencies, hospice care, outpatient services, skilled nursing facilities, community clinics and physician organizations throughout California and in parts of Texas and New Mexico.

On February 14, 2012, SJH reported to OCR that certain files it created for its participation in the meaningful use program, which contained ePHI, were publicly accessible on the internet from February 1, 2011, until February 13, 2012, via Google and possibly other internet search engines. The server SJH purchased to store the files included a file sharing application whose default settings allowed anyone with an internet connection to access them. Upon implementation of this server and the file sharing application, SJH did not examine or modify it. As a result, the public had unrestricted access to PDF files containing the ePHI of 31,800 individuals, including patient names, health statuses, diagnoses, and demographic information.

OCR's investigation indicated the following potential violations of the HIPAA Rules:

- SJH potentially disclosed the PHI of 31,800 individuals;
- Evidence indicated that SJH failed to conduct an evaluation in response to the environmental and operational changes presented by implementation of a new server for its meaningful use project, thereby compromising the security of ePHI; and
- Although SJH hired a number of contractors to assess the risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by SJH, evidence indicated that

this was conducted in a patchwork fashion and did not result in an enterprise-wide risk analysis, as required by the HIPAA Security Rule.

In addition to the $2.14 million settlement, SJH agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop and implement a risk management plan;
- Revise its use and disclosure of protected health information policies and procedures; and
- Train its staff on these revised policies and procedures.

This settlement occurred in October of 2016.

Resolution Agreement with University of Massachusetts Amherst

The University of Massachusetts Amherst (UMass) agreed to settle potential violations of the HIPAA Privacy and Security Rules. The settlement includes a corrective action plan and a monetary payment of $650,000, which is reflective of the fact that the University operated at a financial loss in 2015.

On June 18, 2013, UMass reported to OCR that a workstation in its Center for Language, Speech, and Hearing (the "Center") was infected with a malware program, which resulted in the impermissible disclosure of ePHI of 1,670 individuals, including names, addresses, Social Security numbers, dates of birth, health insurance information, diagnoses and procedure codes. The University determined that the malware was a generic remote access Trojan horse that infiltrated their system, providing impermissible access to ePHI, because UMass did not have a firewall in place.

OCR's investigation indicated the following potential violations of the HIPAA Rules:

- UMass had failed to designate all of its health care components when hybridizing, incorrectly determining that, while its University Health Services was a covered health care component, other components, including the Center where the breach of ePHI occurred, were not covered components.[11] Because UMass failed to designate the Center a health care component, UMass did not implement policies and procedures at the Center to ensure compliance with the HIPAA Privacy and Security Rules.
- UMass failed to implement technical security measures at the Center to guard against unauthorized access to ePHI transmitted over an electronic communications network by ensuring that firewalls were in place at the Center.
- Finally, UMass did not conduct an accurate and thorough risk analysis until September 2015.

In addition to the monetary settlement, UMass agreed to a corrective action plan that requires the organization to:

[11] The HIPAA Privacy Rule permits legal entities that have some functions that are covered by HIPAA, and some that are not, to elect to become a "hybrid entity." To successfully "hybridize," the entity must designate in writing the health care component(s) and include those components of the entity that perform HIPAA-covered functions and business associate functions, and assure HIPAA compliance for its covered health care components.

- Conduct an enterprise-wide risk analysis;
- Develop and implement a risk management plan;
- Revise its policies and procedures for the HIPAA Privacy Rule and Breach Notification Rule; and
- Train its staff on these revised policies and procedures.

This settlement occurred in November of 2016.

Resolution Agreement with Presence Health

Presence Health agreed to settle potential violations of the HIPAA Breach Notification Rule with OCR. Presence paid $475,000 and agreed to adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. Presence Health is one of the largest health care networks serving Illinois and consists of approximately 150 locations, including 11 hospitals and 27 long-term care and senior living facilities. Presence also has multiple physicians' offices and health care centers in its system, and offers home care, hospice care, and behavioral health services.

On January 31, 2014, OCR received a breach notification report from Presence indicating that, on October 22, 2013, Presence discovered that paper-based operating room schedules, which contained the PHI of 836 individuals, were missing from the Presence Surgery Center at the Presence St. Joseph Medical Center in Joliet, Illinois. The information consisted of the affected individuals' names, dates of birth, medical record numbers, dates of procedures, types of procedures, surgeon names, and types of anesthesia. OCR's investigation revealed that Presence Health failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the 836 individuals affected by the breach, prominent media outlets (as required for breaches affecting 500 or more individuals), and OCR.

In addition to the $475,000 settlement amount, the agreement requires Presence to:

- To revise its policies and procedures to comply with the Breach Notification Rule;
- Explicitly delineate its workforce members roles and responsibilities for receiving and addressing internal and external reports involving the potential breach of PHI;
- Train its workforce members; and
- To revise its policies for sanctioning employees who fail to comply with its policies and procedures for implementing the Breach Notification Rule.

This settlement occurred in January of 2017.

Resolution Agreement with MAPFRE Life Insurance Company

MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules with OCR. MAPFRE paid $2.2 million and agreed to adopt a corrective action plan to correct deficiencies with its HIPAA

compliance program. MAPFRE is a subsidiary company of MAPFRE S.A., a global multinational insurance company headquartered in Spain. MAPFRE underwrites and administers a variety of insurance products and services in Puerto Rico, including personal and group health insurance plans.

On September 29, 2011, MAPFRE filed a breach report with OCR indicating that a USB data storage device containing ePHI was stolen from its IT department, where the device was left without safeguards. According to the report, the USB data storage device included complete names, dates of birth and Social Security numbers. The report noted that the breach affected 2,209 individuals. MAPFRE informed OCR that it was able to identify the breached ePHI by reconstituting the data on the computer on which the USB data storage device was attached.

OCR's investigation revealed MAPFRE's noncompliance with the HIPAA Rules, specifically a failure to conduct its risk analysis and implement risk management plans, contrary to its prior representations. In addition, MAPFRE failed to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September 1, 2014. MAPFRE also failed to implement or delayed implementing other corrective measures it informed OCR it would undertake. In addition to the $2.2 million settlement amount, the agreement requires MAPFRE to:

- Develop a comprehensive corrective action plan;
- Conduct a thorough risk analysis and implement a risk management plan; and
- Train its workforce members.

This settlement occurred in January of 2017.

Civil Money Penalty involving Children's Medical Center of Dallas

Children's Medical Center of Dallas (Children's) impermissibly disclosed electronic protected health information (ePHI) and was found to be in non-compliance with multiple standards of the HIPAA Security Rule. OCR issued a Notice of Proposed Determination in accordance with 45 CFR 160.420, which included instruction for how Children's could file a request for a hearing. Children's did not request a hearing. Accordingly, OCR issued a Notice of Final Determination, and Children's paid the full civil money penalty of $3.2 million. Children's is a pediatric hospital in Dallas, Texas, and is part of Children's Health, the seventh largest pediatric health care provider in the nation.

On January 18, 2010, Children's filed a breach report with OCR indicating the loss of an unencrypted, non-password protected BlackBerry device at the Dallas/Fort Worth International Airport on November 19, 2009. The device contained the ePHI of approximately 3,800 individuals. On July 5, 2013, Children's filed a separate HIPAA Breach Notification Report with OCR, reporting the theft of an unencrypted laptop from its premises sometime between April 4 and April 9, 2013. Children's reported that the device contained the ePHI of 2,462 individuals. Although Children's implemented some physical safeguards to the laptop storage area (e.g., badge access and a security camera at one of the entrances), it also provided access to the area to workforce not authorized to access ePHI.

OCR's investigation revealed Children's noncompliance with HIPAA Rules, specifically, a failure to implement risk management plans, contrary to prior external recommendations to do so, and a failure to deploy encryption or an equivalent alternative measure on all of its laptops, work stations, mobile devices and removable storage media until April 9, 2013. Despite Children's knowledge about the risk of maintaining unencrypted ePHI on its devices as far back as 2007, Children's issued unencrypted BlackBerry devices to nurses and allowed its workforce members to continue using unencrypted laptops and other mobile devices until 2013.

This CMP was imposed in January of 2017.

Resolution Agreement with Memorial Healthcare System

Memorial Healthcare System (MHS) paid $5.5 million to settle potential violations of the HIPAA Privacy and Security Rules with OCR. MHS agreed to adopt a corrective action plan. MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

MHS reported to OCR that the protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and Social Security numbers. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

In addition to the $5,500,000 settlement amount, MHS is required to complete a risk analysis and risk management plan that includes:

- All identified risks and vulnerabilities identified at MHS related to enterprise-wide PHI security;
- Evidence that MHS has implemented and maintains a risk management plan to address such risks and vulnerabilities and expected dates of implementation; and
- Revision of its policies and procedures regarding information system activity review which requires the regular review of audit logs, access reports, and security incident tracking reports. In addition, the policies and procedures will address computer system access establishment, modification and termination.

This settlement occurred in February of 2017.

Resolution Agreement with Metro Community Provider Network

Metro Community Provider Network (MCPN) agreed to settle charges that it potentially violated the HIPAA Security Rules, based on the lack of a security management process to safeguard electronic protected health information (ePHI). MCPN is a federally qualified health center (FQHC). MCPN provides primary medical care, dental care, pharmacies, social work, and behavioral health care services throughout the greater Denver, Colorado metropolitan area to approximately 43,000 patients per year, a large majority of whom have incomes at or below the poverty level.

On January 27, 2012, MCPN filed a breach report with OCR, indicating that a hacker accessed employees' email accounts and obtained 3,200 individuals' ePHI through a phishing incident. OCR's investigation revealed that MCPN took necessary corrective action related to the phishing incident; however, the investigation also revealed that MCPN failed to conduct a risk analysis until mid-February 2012. Prior to the breach incident, MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in its ePHI environment, and, consequently, had not implemented any corresponding risk management plans to address the risks and vulnerabilities identified in a risk analysis. When MCPN finally conducted a risk analysis, that risk analysis, as well as all subsequent risk analyses, were insufficient to meet the requirements of the Security Rule.

In addition to the $400,000 settlement amount, the agreement requires MCPN to:

- Develop a comprehensive corrective action plan;
- Conduct a thorough risk analysis and implement a risk management plan; and
- Train its workforce members.

This settlement occurred in April of 2017.

Resolution Agreement with the Center for Children's Digestive Health

The Center for Children's Digestive Health (CCDH) agreed to settle potential violations of the HIPAA Privacy Rule with OCR. CCDH is a small, for-profit health care provider with a pediatric subspecialty practice that operates its practice in seven clinic locations in Illinois.

In August 2015, OCR initiated a compliance review of CCDH following an initiation of an investigation of a business associate, FileFax, Inc., which stored records containing protected health information (PHI) for CCDH. While CCDH began disclosing PHI to Filefax in 2003, neither party could produce a signed Business Associate Agreement (BAA) prior to Oct. 12, 2015.

In addition to the $31,000 settlement amount, the agreement requires CCDH to:

- Develop and implement a corrective action plan to address HIPAA Privacy Rule requirements regarding the contents and requirements of business associate agreements;
- Revise its policies and procedures; and

- Train its workforce members.

This settlement occurred in April of 2017.

Resolution Agreement with CardioNet

CardioNet agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. CardioNet impermissibly disclosed the unsecured electronic protected health information (ePHI) of 1,391 individuals. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January 2012, CardioNet reported to OCR that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania-based organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

In addition to the $2.5 million settlement amount, the agreement requires CardioNet to:

- Develop a corrective action plan an conduct a risk analysis of security risks, threats, and vulnerabilities enterprise-wide;
- Revise its policies and procedures governing the removal of hardware and electronic media into and outside of its facilities as well as the encryption of hardware and electronic media;
- Revise its training materials; and
- Train its workforce members.

This settlement occurred in April of 2017.

Resolution Agreement with Memorial Hermann Health System

Memorial Hermann Health System (MHHS) agreed to pay $2.4 million to settle potential violations of the HIPAA Privacy Rule with OCR. MHHS is a not-for-profit health system located in Southeast Texas, comprised of 16 hospitals and specialty services in the Greater Houston area.

OCR initiated a compliance review of MHHS based on multiple media reports suggesting that MHHS disclosed a patient's protected health information (PHI) without an authorization. In September 2015, a patient at one of MHHS's clinics presented an allegedly fraudulent identification card to office staff. The staff immediately alerted appropriate authorities of the incident, and the patient was arrested. This disclosure of PHI to law enforcement was permitted under the HIPAA Rules. However, MHHS subsequently published a press release concerning

the incident in which MHHS senior management approved the impermissible disclosure of the patient's PHI by adding the patient's name in the title of the press release. In addition, MHHS failed to timely document the sanctioning of its workforce members for impermissibly disclosing the patient's information.

In addition to a $2.4 million monetary settlement, a corrective action plan requires MHHS to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members. The corrective action plan also requires all MHHS facilities to attest to their understanding of permissible uses and disclosures of PHI, including disclosures to the media.

This settlement occurred in April of 2017.

Resolution Agreement with St. Luke's – Roosevelt Hospital Center

St. Luke's-Roosevelt Hospital Center Inc. (St. Luke's) paid OCR $387,200 to settle potential violations of the HIPAA Privacy Rule and agreed to implement a comprehensive corrective action plan. St. Luke's operates the Institute for Advanced Medicine, formerly Spencer Cox Center for Health (the Spencer Cox Center), which provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases. St. Luke's is 1 of 7 hospitals that comprise the Mount Sinai Health System (MSHS).

In September 2014, OCR received a complaint alleging that a staff member from the Spencer Cox Center impermissibly disclosed the complainant's protected health information (PHI) to the complainant's employer. This impermissible disclosure included sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse. OCR's subsequent investigation revealed that staff at the Spencer Cox Center impermissibly faxed the patient's PHI to his employer rather than sending it to the requested personal post office box. Additionally, OCR discovered that the Spencer Cox Center was responsible for a related breach of sensitive information that occurred nine months prior to the aforementioned incident, but had not addressed the vulnerabilities in their compliance program to prevent impermissible disclosures.

In addition to the settlement amount, St. Luke's agreed to:

- Develop a corrective action plan to address the release of protected health information;
- Revise its policies and procedures regarding the uses and disclosures of protected health information; and
- Update its training materials and train its workforce members.

This settlement occurred in May of 2017.

Resolution Agreement with 21st Century Oncology

21st Century Oncology, Inc. (21CO) agreed to pay $2.3 million in lieu of potential civil money penalties to OCR to settle potential violations of the HIPAA Privacy and Security Rules. 21CO

is a provider of cancer care services and radiation oncology. With their headquarters located in Fort Myers, Florida, 21CO operates and manages 179 treatment centers, including 143 centers located in 17 states and 36 centers located in seven countries in Latin America.

On two separate occasions in 2015, the Federal Bureau of Investigation (FBI) notified 21CO that patient information was illegally obtained by an unauthorized third party and produced 21CO patient files purchased by an FBI informant. As part of its internal investigation, 21CO determined that the attacker may have accessed 21CO's network SQL database as early as October 3, 2015, through the remote desktop protocol from an exchange server within 21CO's network. 21CO determined that 2,213,597 individuals were affected by the impermissible access to their names, Social Security numbers, physicians' names, diagnoses, treatment, and insurance information. OCR's subsequent investigation revealed that 21CO failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information (ePHI); failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and disclosed protected health information (PHI) to third party vendors without a written business associate agreement.

In addition to the $2.3 million monetary settlement, a corrective action plan requires 21CO to:

- Complete a risk analysis and risk management plan to assess threats and mitigate harm involving risks and vulnerabilities among its information systems;
- Revise policies and procedures;
- Educate its workforce members on revised policies and procedures;
- Provide all maintained business associate agreements to OCR; and
- Submit an internal monitoring plan to OCR.

This settlement occurred in December of 2017.

On May 25, 2017, 21CO filed for Chapter 11 bankruptcy protection in the United States Bankruptcy Court for the Southern District of New York. The settlement with OCR will resolve OCR's claims against 21CO, and the corrective action plan will ensure that the reorganized entity emerges from bankruptcy with a strong HIPAA compliance program in place. The settlement with OCR was approved by the Bankruptcy Court on December 11, 2017.