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

For Calendar Years 2013 and 2014

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 and security 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. 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;
- 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 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 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 such provisions for the following year.

[1] As with the first Report to Congress, this Report covers a two-year period, allowing the Department to better compare trends and outcomes from one year to the next, in addition to providing cumulative data. Covering a two-year period also aligns the timing of this Report with the Report to Congress on Breaches of Unsecured Protected Health Information.

This report is prepared for calendar years 2013 and 2014. The Reports to Congress on Compliance with the HIPAA Privacy and Security Rules for previous years are available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereptmain.html.

Background

HIPAA was enacted on August 21, 1996. Subtitle F of HIPAA, known as the Administrative Simplification provisions, among other things, required the Secretary to establish standards for the privacy and security of individually identifiable health information held by an entity covered by 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 that provides certain services to or performs functions on behalf of a covered entity, or another business associate of a covered entity, that require access to protected health information (PHI).

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

[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. 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.

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 both since their respective compliance dates, as well as specifically with regard to calendar years 2013 and 2014.

Enforcement Process

OCR enforces the HIPAA Rules by investigating written complaints filed with OCR, either on paper, by e-mail, or through our complaint portal, and by conducting compliance reviews with regard to circumstances brought to the attention of OCR by other means, 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.

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.

- 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: 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. Further, in many cases, OCR provides technical

[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.

[4] Section 13411 of the HITECH Act, which became effective on February 17, 2010, authorizes and requires the Department to provide for 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 currently underway.

assistance to the covered entity or business associate to resolve the case quickly without further investigation.

OCR may open compliance reviews of covered entities and business associates based on an event or incident brought to the attention of OCR by means other than a complaint, such as through a breach report. Once OCR initiates either a complaint investigation or a compliance review, OCR then gathers evidence, including witness statements, information from site visits, or various types of documents, from the parties to the complaint or compliance review. 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 then 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 must obtain 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.

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 civil money penalty (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 possible CMPs for which the covered entity or business associate is 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.

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 an agreement that is satisfactory to OCR 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 by notifying 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 2014, out of all the cases OCR attempted to resolve informally through a resolution agreement, only one case has resulted in the imposition of a CMP.[5]

Enforcement Data

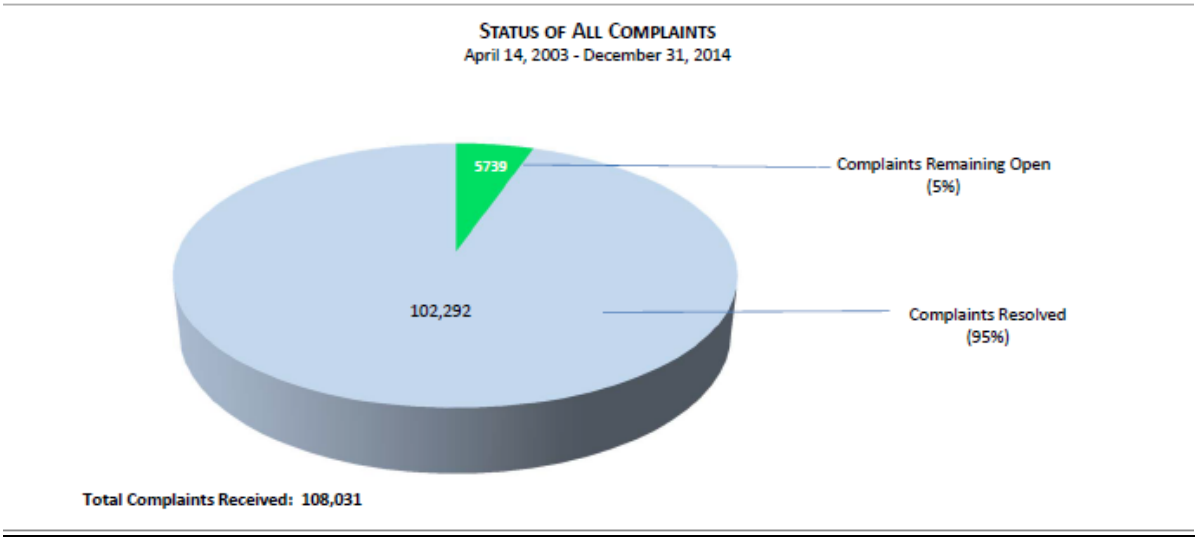
Cumulative Data

The following section provides an overview of the cumulative enforcement data through the end of calendar year 2014, followed by specific enforcement data for calendar years 2013 and 2014.

Complaints Received and Closed

From April 14, 2003, the compliance date of the HIPAA Privacy Rule (the date used to determine cumulative numbers because it was the first compliance date of all of the HIPAA Rules), to December 31, 2014, OCR received 108,031 complaints alleging violations of the HIPAA Rules. As of December 31, 2014, OCR resolved 102,292, or ninety-five percent, of the complaints received. The majority of complaints received are resolved within one year of their receipt. The remaining open cases, 5,739, or five percent, carried over into 2015.

[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 60,529, or fifty-nine percent, of the resolved cases, 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 23,314, or twenty-three present, of the resolbed cases, OCR required the covered entity or business associate to take corrective action. In 10,566, or ten percent, of the resolved cases, OCR found no violation had occurred. Finally, in the remaining 7,883 cases, or eight percent, OCR provided technical assistance or took some other action to resolve the cases.

Investigated Resolutions

As outlined above, OCR can only investigate complaints against HIPAA covered entities and business associates that are timely filed and allege a violation of the HIPAA Rules.

From 2003 to 2014, OCR investigated 33,880 complaints. Of those, OCR resolved 23,314, or sixty-nine percent, of the cases by requiring covered entities and business associates to take corrective actions and/or provided technical assistance to covered entities and business associates to resolve indications of noncompliance and to achieve change in compliance. Corrective actions taken by covered entities and business associates include: correcting any problems indicated by the evidence in the investigation; training employees; sanctioning employees; revising policies and procedures; and mitigating any alleged harm. The goal of requiring corrective action is systemic change in the covered entity's or business associate's policies and actions to ensure the proper protection of health information of individuals served by the entity. Specific information about the major cases involving resolution agreements follows below. In the other 10,566, or thirty-one percent, of the cases investigated, OCR found that no violation of the HIPAA Rules occurred.

Compliance Reviews

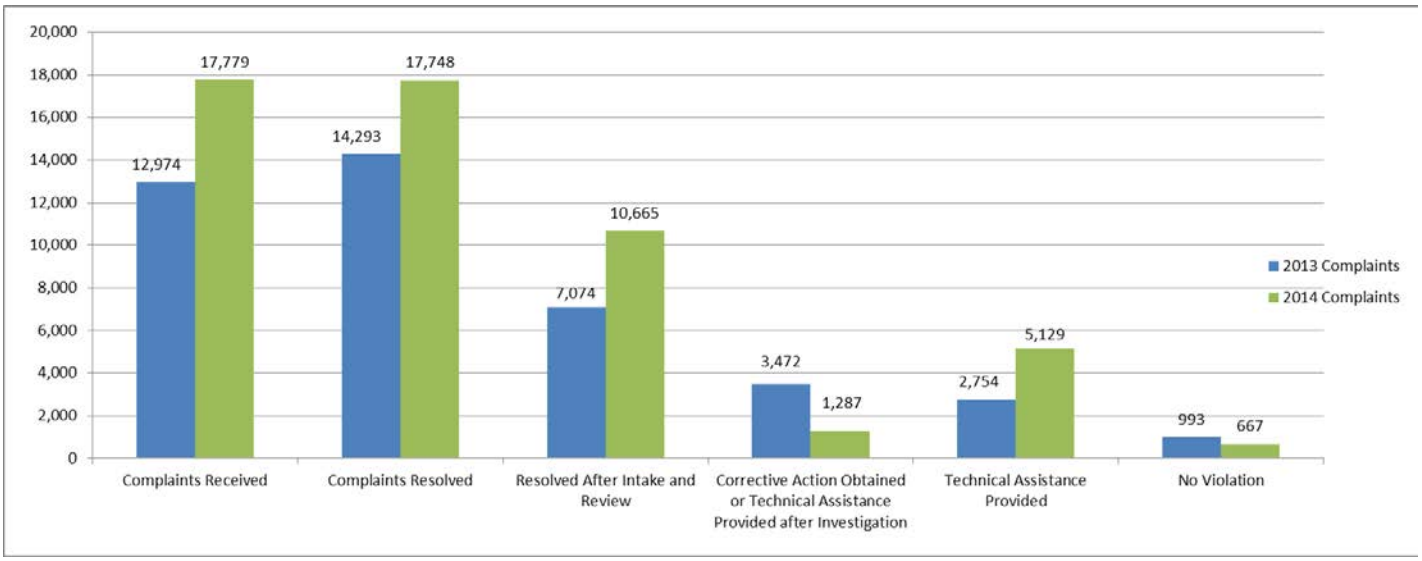
OCR conducts compliance reviews of covered entities and business associates based on events or incidents brought to the attention of OCR by means other than a complaint, such as through a breach report. This includes conducting investigations into all reports of breaches affecting 500 or more individuals, as well as some reports of breaches affecting fewer than 500 individuals. From 2003 to 2014, OCR opened 1,625 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 1,153 compliance reviews were opened as a result of a breach report affecting 500 or more individuals.

Issues and Entities

From 2003 to 2014, the compliance issues investigated most by OCR, compiled cumulatively in order of frequency, are: impermissible uses and disclosures of PHI; lack of safeguards for PHI; denial of individuals' access to their PHI; lack of administrative safeguards of ePHI, and uses or disclosures of more than the minimum necessary PHI. The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance with regard to the Privacy Rule, in order of frequency, are: private practices; general hospitals; outpatient facilities; pharmacies, and health plans, which include group health plans and health insurance issuers.

2013 and 2014 Data

2013 and 2014 Complaints and Compliance Reviews

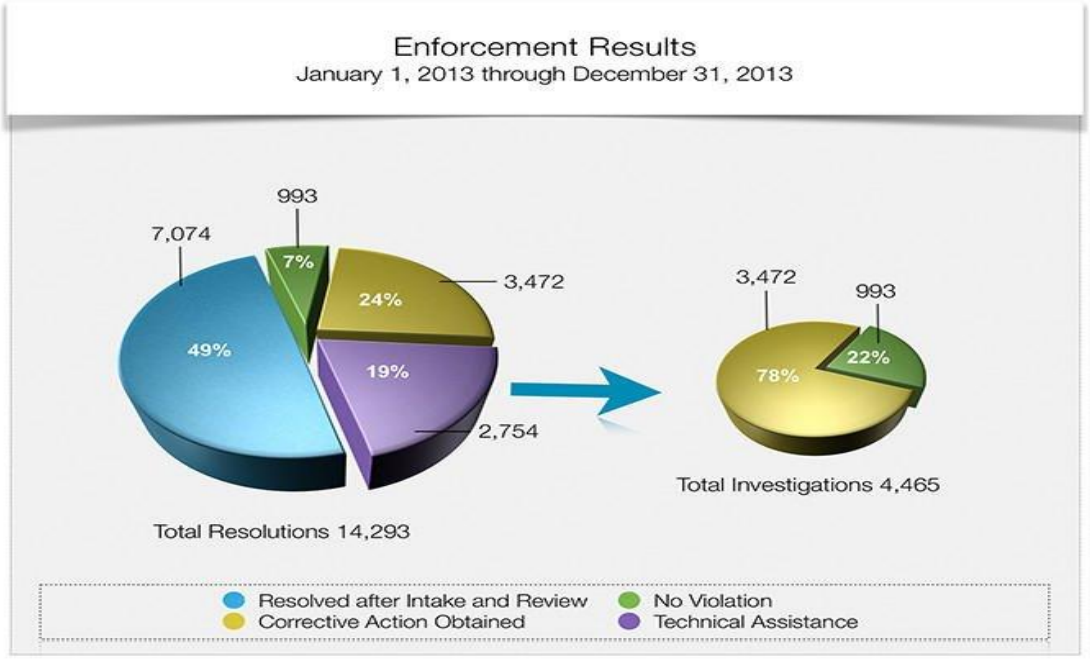


2013 Complaints and Compliance Reviews

Although OCR resolved over ninety-one percent of the complaints received since the compliance dates of the HIPAA Rules by the end of calendar year 2012, a remainder of approximately[6] 6,931 open complaints carried over into calendar year 2013. During calendar year 2013, OCR received an additional 12,974 complaints, representing the largest number of complaints received in any calendar year to that point, and an increase of 2,517 complaints from 2012. OCR resolved a total of 14,293, or seventy-two percent, of complaints in 2013.

In 7,074, or forty-nine percent, of complaints, 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 2,754, or nineteen percent, of the complaints investigated in 2013, OCR provided technical assistance to the covered entity or business associate. In 3,472, or twenty-four percent, of the complaints investigated, after investigation OCR provided technical assistance or required the covered entity or business associate to take corrective action. In 993, or seven percent, of the complaints investigated, OCR found that no violation of the HIPAA Rules had occurred.

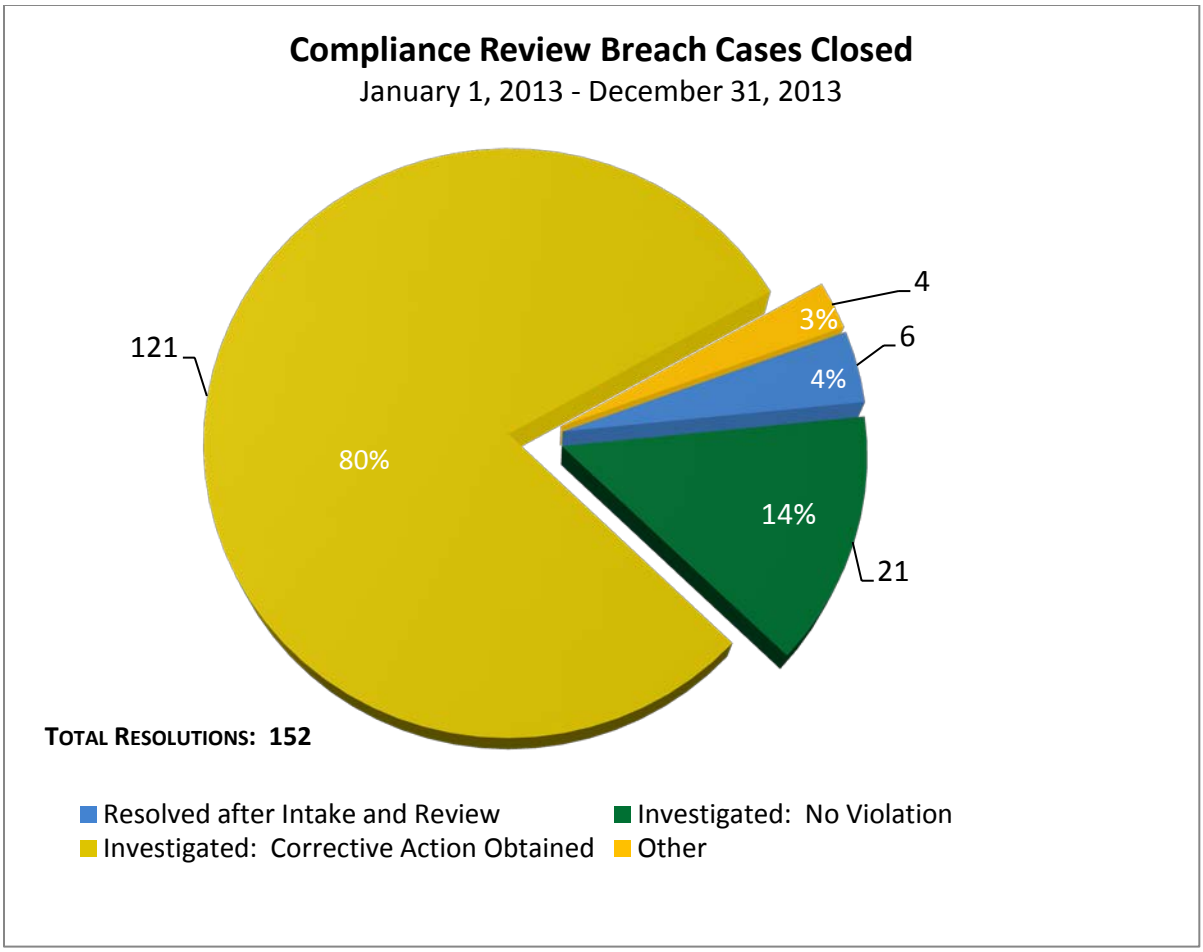
[6] OCR's investigatory case processing system is a live system, in which the inventory of cases fluctuates depending on the case information entered by the staff in the ten regional offices and in headquarters. The numbers provided in this report reflect the most current information in the system when the report was prepared.



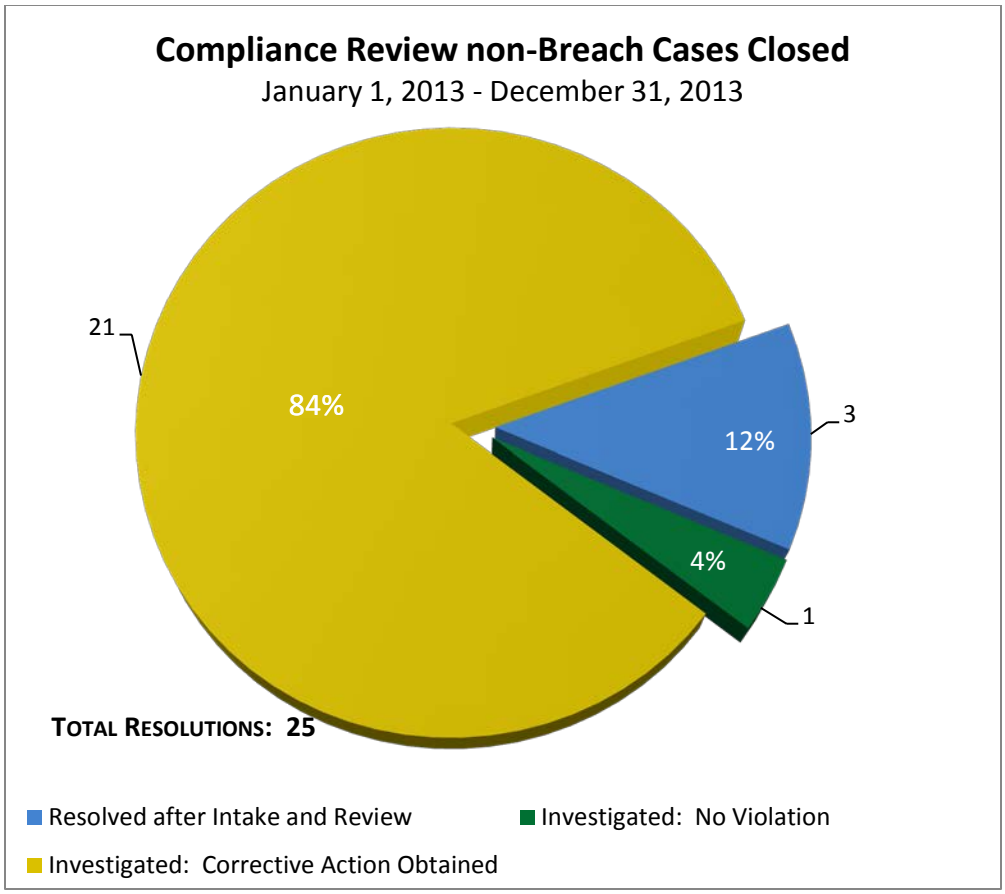
During calendar year 2013, OCR opened at least 445 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 257 reviews were opened as a result of breach reports affecting 500 or more individuals.[7]

OCR closed 152 breach compliance reviews in 2013. In 121, or eighty percent, of the breach compliance reviews completed in 2013, OCR required the covered entity or business associate to take corrective action. In 21, or fourteen percent, of the breach compliance reviews completed, OCR found that no violation of the HIPAA Rules had occurred. In four, or three percent, of the compliance reviews completed, OCR closed the breach compliance review without requiring actions or making recommendations, 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. Finally, in six, or four percent, of the breach compliance reviews completed, OCR determined that it did not have jurisdiction under the HIPAA Rules to investigate the allegations 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.

[7] As mentioned previously in the report, compliance reviews are opened for all reports of breaches affecting 500 or more individuals. Additionally, compliance reviews are opened for some reports of breaches affecting fewer than 500 individuals.



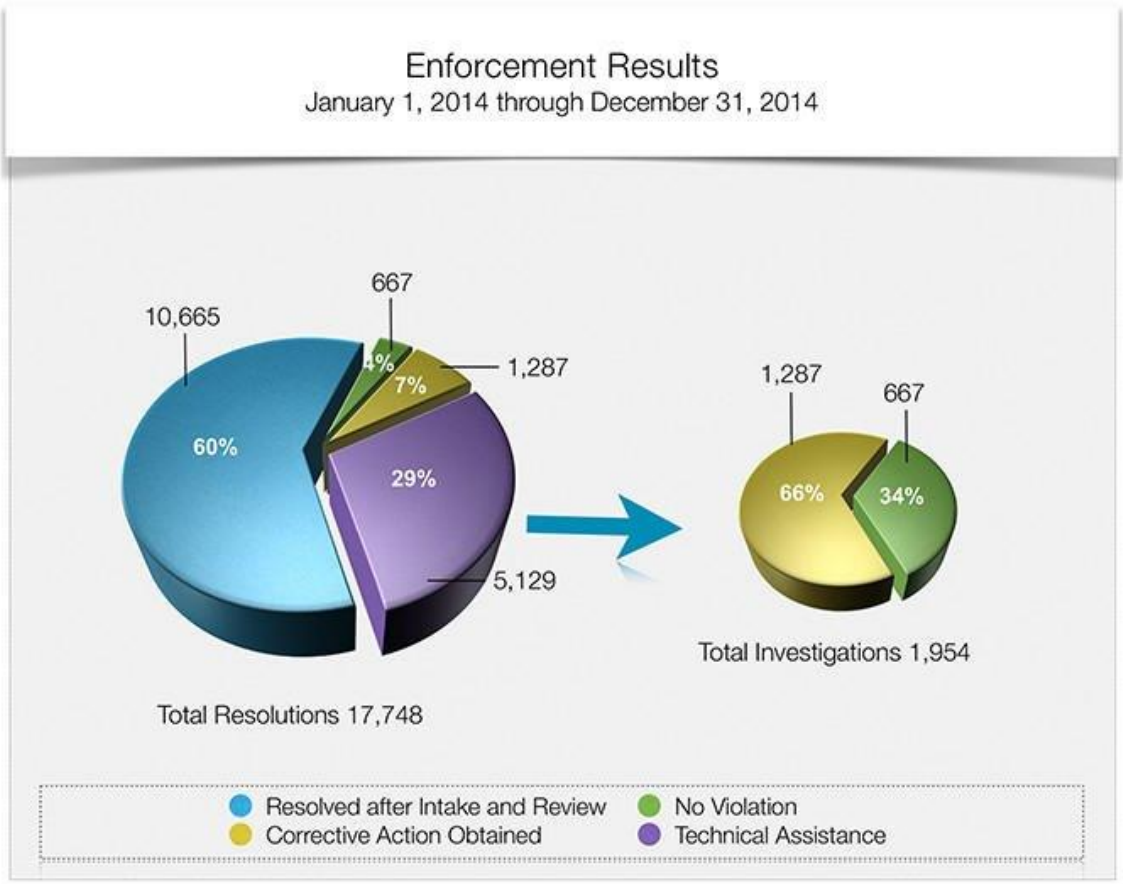
In 21, or eighty-four percent, of the non-breach compliance reviews completed in 2013, OCR required the covered entity or business associate to take corrective action. In one, or four percent of the non- breach compliance reviews completed, OCR found that no violation of the HIPAA Rules had occurred. Finally, in three, or twelve percent, of the non-breach compliance reviews completed, OCR determined that it did not have jurisdiction under the HIPAA Rules to investigate the allegations 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.



2014 Complaints and Compliance Reviews

Although OCR resolved over ninety-four percent of the complaints received since the compliance dates of the HIPAA Rules by the end of calendar year 2013, a remainder of approximately 5,447 open complaints carried over into calendar year 2014. During calendar year 2014, OCR received an additional 17,779 complaints, a significant increase of 4,805 complaints over the previous year's all-time high. OCR resolved a total of 17,748 complaints.

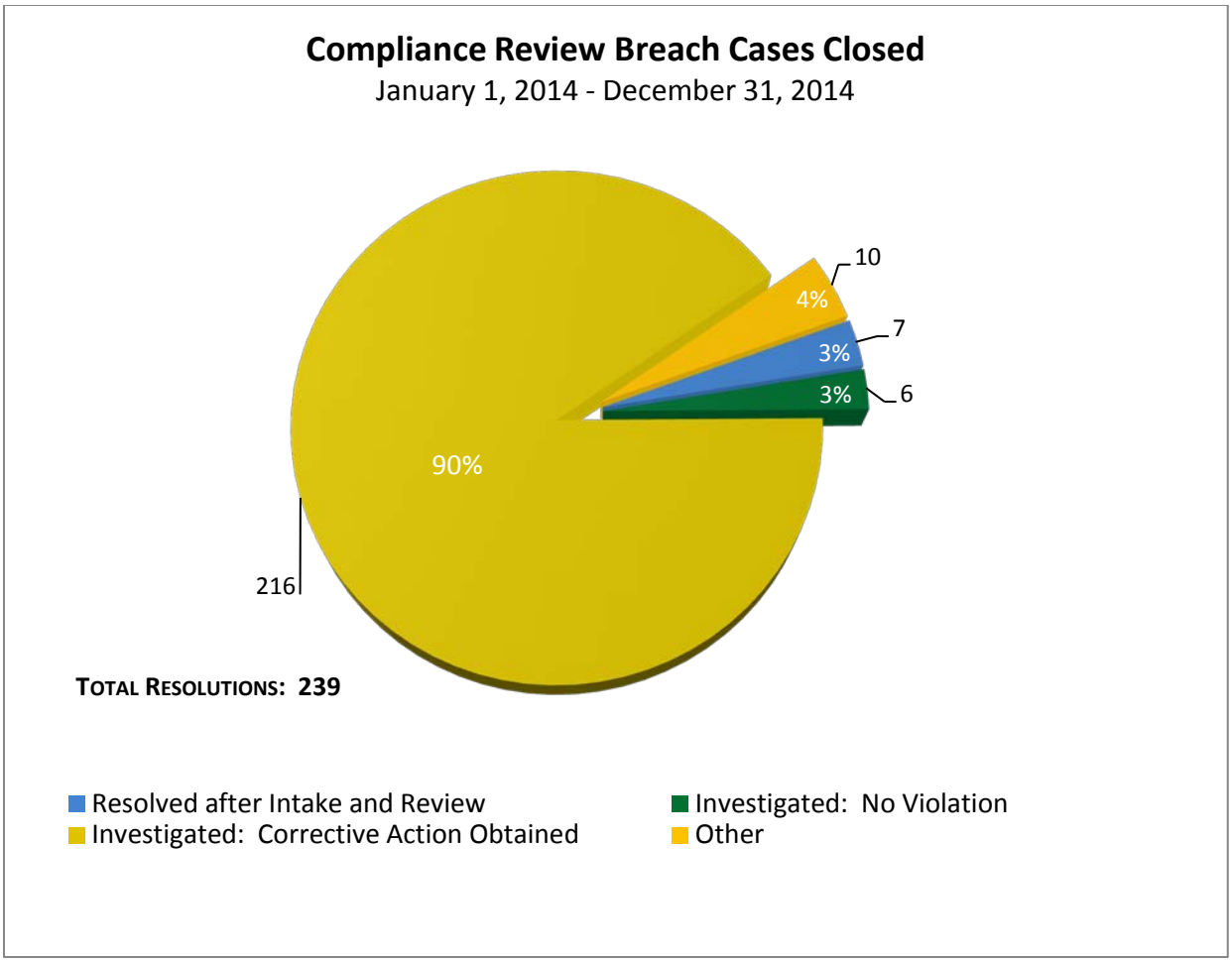
In 5,129, or twenty-nine percent, of the complaints investigated in 2014, OCR provided technical assistance to the covered entity or business associate. In 1,287, or seven percent, of the complaints investigated, after investigation OCR provided technical assistance to the covered entity or business associate or required the covered entity or business associate to take corrective action. In 667, or four percent, of the complaints investigated, OCR found that no violation of the HIPAA Rules had occurred. Finally, in 10,665, or sixty percent, of the complaints, 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.



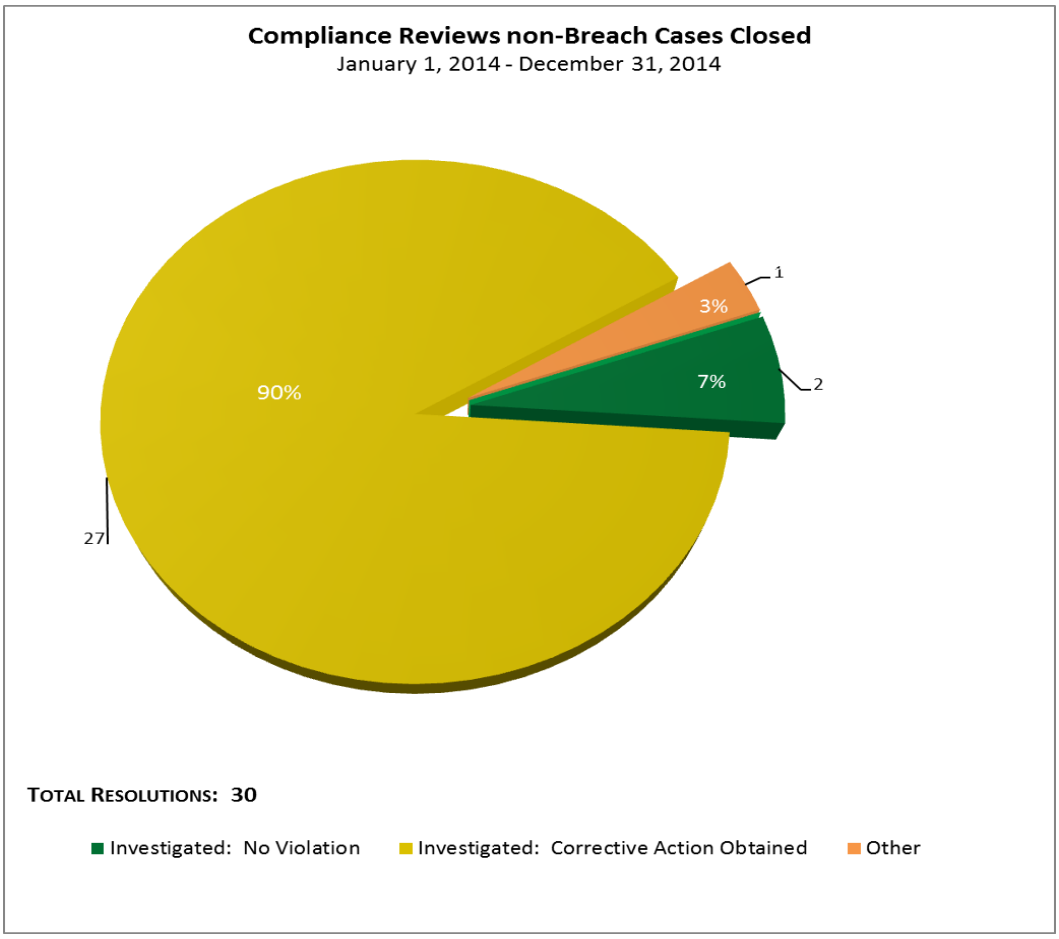
During calendar year 2014, OCR opened at least 507 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 285 compliance reviews were opened as a result of a breach report affecting 500 or more individuals.[8]

OCR closed 239 breach compliance reviews in 2014. In 216, or ninety percent, of the breach compliance reviews completed in 2014, OCR required the covered entity or business associate to take corrective action. In six, or three percent, of the breach compliance reviews completed, OCR found that no violation of the HIPAA Rules had occurred. In ten, or four percent, of the breach compliance reviews completed, OCR closed the breach compliance review without requiring actions or making recommendations. Finally, in seven, or three percent, of the breach compliance reviews completed, OCR determined that it did not have jurisdiction under the HIPAA Rules to investigate the allegations 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.

[8] *Id*.



In 27, or ninety percent, of the non-breach compliance reviews completed in 2014, OCR required the covered entity or business associate to take corrective action. In two, or seven percent, of the non- breach compliance reviews completed, OCR found that no violation of the HIPAA Rules had occurred. Finally, in one, or three percent, of the non-breach compliance reviews completed, OCR determined that it did not have jurisdiction under the HIPAA Rules to investigate the allegations 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.



Significant Activities: Resolution Agreements, CMPs, and Subpoenas[9] in 2013 and 2014

Resolution Agreements

Resolution Agreement with Idaho State University

Idaho State University (ISU) agreed to pay $400,000 to settle alleged violations of the HIPAA Security Rule. The settlement involved the breach of unsecured electronic protected health information (ePHI) of approximately 17,500 patients at ISU's Pocatello Family Medicine Clinic.

OCR opened an investigation after ISU notified OCR of the breach in which the ePHI of approximately 17,500 patients was unsecured for at least 10 months, due to the disabling of firewall protections at servers maintained by ISU. OCR's investigation indicated that ISU's risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities. ISU also failed to assess the likelihood of potential risks occurring.

[9] Information provided here on Resolution Agreements, Civil Money Penalties (CMPs), and Subpoenas is based on the year in which the Agreement was signed, the CMP assessed, or the Subpoena issued. In addition, the cases were begun in years prior to 2013 and 2014 .

OCR concluded that ISU did not apply proper security measures and policies to address risks to ePHI and did not have procedures for routine review of their information system in place, which could have detected the firewall breach much sooner. ISU agreed to a comprehensive corrective action plan (CAP) to address the issues uncovered by the investigation and its failure to ensure uniform implementation of required HIPAA Security Rule protections at each of its covered clinics, which included:

- implementing ongoing and routine security measures to protect enterprise-wide information systems;
- implementing and disseminating policies and procedures for the safeguarding of PHI to all workforce members; and
- training its workforce members.

Resolution Agreement with Shasta Regional Medical Center

Shasta Regional Medical Center (SRMC) agreed to a comprehensive corrective action plan to settle potential violations of the HIPAA Privacy Rule.

OCR opened a compliance review of SRMC following a Los Angeles Times article which indicated two SRMC senior leaders had met with media to discuss medical services provided to a patient. OCR's investigation indicated that SRMC failed to safeguard the patient's protected health information (PHI) from impermissible disclosure by intentionally disclosing PHI to multiple media outlets on at least three separate occasions, without a valid written authorization. OCR's review indicated that senior management at SRMC impermissibly shared details about the patient's medical condition, diagnosis and treatment in an email to the entire workforce. In addition, SRMC failed to sanction its workforce members for impermissibly disclosing the patient's records pursuant to its internal sanctions policy.

In addition to a $275,000 monetary settlement, a corrective action plan (CAP) requires SRMC to:

- update its policies and procedures on safeguarding PHI from impermissible uses and disclosures; and
- train its workforce members.

The CAP also requires fifteen other hospitals or medical centers under the same ownership or operational control as SRMC to attest to their understanding of permissible uses and disclosures of PHI, including disclosures to the media.

Resolution Agreement with WellPoint

The managed care company WellPoint Inc. agreed to pay $1.7 million to settle potential violations of the HIPAA Privacy and Security Rules. This case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet.

OCR began its investigation following a breach report submitted by WellPoint that indicated that security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet.

OCR's investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule.

The investigation indicated WellPoint did not:

- adequately implement policies and procedures for authorizing access to the on-line application database;
- perform an appropriate technical evaluation in response to a software upgrade to its information systems; and
- have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.

As a result, beginning on Oct. 23, 2009, until Mar. 7, 2010, the investigation indicated that WellPoint impermissibly disclosed the ePHI of 612,402 individuals by allowing access to the ePHI of such individuals maintained in the application database. This data included names, dates of birth, addresses, Social Security numbers, telephone numbers and health information. Whether systems upgrades are conducted by covered entities or their business associates, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the Internet.

Resolution Agreement with Affinity Health Plan

Affinity Health Plan, Inc. agreed to settle potential violations of the HIPAA Privacy and Security Rules for $1,215,780. Affinity Health Plan is a not-for-profit managed care plan serving the New York metropolitan area.

Affinity filed a breach report with OCR on April 15, 2010, that indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

Affinity estimated that up to 344,579 individuals may have been affected by this breach. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to:

- use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent;
- conduct a comprehensive risk analysis of the ePHI security risk and vulnerabilities that incorporates all electronic equipment and systems; and
- develop a plan to address and mitigate any security risks and vulnerabilities discovered.

Resolution Agreement with Adult & Pediatric Dermatology of Massachusetts

Adult & Pediatric Dermatology, P.C., of Concord, Mass., (APDerm) agreed to pay $150,000 to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules. APDerm is a private practice that delivers dermatology services in four locations in Massachusetts and two in New Hampshire. This case was the first settlement with a covered entity for not having policies and procedures in place to address the HIPAA Breach Notification Rule.

OCR opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

In addition to a $150,000 resolution amount, the settlement includes a corrective action plan requiring APDerm to:

- develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities;
- provide an implementation report to OCR.

Resolution Agreement with Skagit County Government

Skagit County, Washington, agreed to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to work closely with the OCR to correct deficiencies in its HIPAA compliance program. Skagit County is located in Northwest Washington, and is home to approximately 118,000 residents. The Skagit County Public Health Department provides essential services to many individuals who would otherwise not be able to afford health care.

OCR opened an investigation of Skagit County upon receiving a breach report that money receipts with electronic protected health information (ePHI) of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server

maintained by the County. OCR's investigation revealed a broader exposure of protected health information involved in the incident, which included the ePHI of 1,581 individuals. Many of the accessible files involved sensitive information, including protected health information concerning the testing and treatment of infectious diseases. OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules.

Skagit County continues to cooperate with OCR through a corrective action plan to ensure it has in place:

- substitute breach notifications for all affected individuals; written policies and procedures;
- documentation requirements;
- training; and
- a process for providing regular status reports to OCR.

Resolution Agreement with QCA Health Plan

QCA Health Plan paid OCR $250,000 to resolve potential violations of the HIPAA Privacy and Security Rules. This enforcement action was publicized with the action below against Concentra Health Services to highlight ongoing industry issues with unencrypted laptop computers and other mobile devices.

OCR received a breach notice in February 2012 from QCA Health Plan, Inc. of Arkansas reporting that an unencrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member's car. While QCA encrypted their devices following discovery of the breach, OCR's investigation revealed that QCA failed to comply with multiple requirements of the HIPAA Privacy and Security Rules, beginning from the compliance date of the Security Rule in April 2005 and ending in June 2012. QCA agreed to a $250,000 monetary settlement and a corrective actions plan that includes:

- an updated risk analysis;
- a corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI;
- retraining of its workforce; and
- documenting its ongoing compliance efforts.

Resolution Agreement with Concentra Health Services

Concentra Health Services paid the OCR $1,725,220 to resolve potential violations of the HIPAA Privacy and Security Rules. This major enforcement action underscores the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield

Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information.

In addition to the payment, Concentra has agreed to adopt a corrective action plan to evidence their remediation of these findings, which includes:

- completing a risk analysis of all systems that contain ePHI; and
- developing a risk management plan that reduces risks and vulnerabilities identified in the risk analysis.

Resolution Agreements with New York and Presbyterian Hospital and Columbia University

OCR entered into settlement agreements with York and Presbyterian Hospital (NYP) and Columbia University (CU), which included resolution amounts totaling $4.8 million. OCR initiated an investigation of NYP and CU following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center." NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing ePHI.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.

In addition to the impermissible disclosure of ePHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.

NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which included:

- undertaking a risk analysis;
- developing a risk management plan;
- revising policies and procedures;
- training staff; and
- providing progress reports to OCR.

Resolution Agreement with Parkview Health System

Parkview Health System, Inc. agreed to settle potential violations of the HIPAA Privacy Rule with OCR. Parkview paid $800,000 and adopted a corrective action plan to address deficiencies in its HIPAA compliance program. Parkview is a nonprofit health care system that provides community-based health care services to individuals in northeast Indiana and northwest Ohio.

OCR opened an investigation after receiving a complaint from a retiring physician alleging that Parkview had violated the HIPAA Privacy Rule. In September 2008, Parkview took custody of medical records pertaining to approximately 5,000 to 8,000 patients while assisting the retiring physician to transition her patients to new providers, and while considering the possibility of purchasing some of the physician's practice. On June 4, 2009, Parkview employees, with notice that the physician was not at home, left 71 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of the physician's home, within 20 feet of the public road and a short distance away from a heavily trafficked public shopping venue.

As a covered entity under the HIPAA Privacy Rule, Parkview must appropriately and reasonably safeguard all protected health information in its possession, from the time it is acquired through its disposition.

Parkview cooperated with OCR throughout its investigation. In addition to the $800,000 resolution amount, the settlement includes a corrective action plan requiring Parkview to:

- revise their policies and procedures;
- train staff; and
- provide an implementation report to OCR.

Resolution Agreement with Anchorage Community Mental Health Services

Anchorage Community Mental Health Services (ACMHS) agreed to settle potential violations of the HIPAA Security Rule with OCR. ACMHS paid $150,000 and adopted a corrective action plan to correct deficiencies in its HIPAA compliance program. ACMHS is a five-facility, nonprofit organization providing behavioral health care services to children, adults, and families in Anchorage, Alaska.

OCR opened an investigation after receiving notification from ACMHS regarding a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals due to

malware compromising the security of its information technology resources. OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

ACMHS cooperated with OCR throughout its investigation and has been responsive to technical assistance provided to date. In addition to the $150,000 settlement amount, the agreement includes a corrective action plan that requires ACMHS to:

- revise and distribute policies and procedures to all workforce members;
- train all workforce members; and
- conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI within its possession.

Subpoenas

OCR did not issue any subpoenas in 2013 or 2014.

Audits

The American Recovery and Reinvestment Act of 2009 (ARRA), in Section 13411 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), requires HHS to perform periodic audits of covered entity and business associate compliance with the Rules.

Audits, unlike complaint investigations or compliance reviews, 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 are to: 1) assess entity compliance efforts with regard to the provisions of 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. The mechanisms by which we plan to achieve these objectives are to analyze an entity's key policies, procedures, and related processes and controls relative to requirements specified in the audit protocol.

The audit program is an important component of OCR's overall health information privacy and security compliance program. OCR uses the audit program to assess HIPAA compliance efforts across a broad range of covered entities and business associates. Audits present an opportunity to examine mechanisms for compliance, identify best practices, and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews. OCR will share best practices learned through the audit process and develop guidance targeted to address compliance challenges uncovered.

Through the use of funds available under HITECH, 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 Price Waterhouse Cooper (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.

In 2014, OCR engaged in preparations for the second phase of the audit program. For example, OCR revised its screening questionnaire intended to gather data about the size, complexity, and operations of potential auditees; this data will help OCR make audit subject selections in a way that is objective and, to the extent possible, representative of a broad cross section of entities covered by HIPAA. OCR also began updating the audit protocol to reflect the new regulatory requirements implemented through the January 25, 2013, Omnibus final rule and to assure that phase 2 of the program could include audits of both covered entities and business associates. Other activities in 2014 included development of additional guidance responsive to issues found through the pilot audits.

OCR launched phase 2 of the audit program in 2016; further details of those audits will be included in subsequent reports.

Ongoing Outreach Efforts to Increase Awareness and Compliance

To effectuate the HITECH Act's mandate to increase education to both HIPAA covered entities and consumers, and to address compliance deficiencies in the regulated community identified by complaint investigations, compliance reviews, and the pilot audit program, OCR significantly built on its existing public outreach and education efforts in 2013 and 2014, with the goal of increasing compliance with the HIPAA Rules across the health care industry. Further, OCR continues to expand its outreach and public education efforts, because such effort offer a systemic means to promote voluntary compliance, and to provide technical assistance to the regulated community before issues occur. OCR's 2013 and 2014 outreach efforts include:

- OCR developed six online training modules that offer free Continuing Medical Education (CME) credits for physicians and Continuing Education (CE) credits for health care professionals via Medscape. The modules offer practical advice on complying with the HIPAA Privacy, Security and Breach Notification Rules, featuring topics such as "EHRs and HIPAA: Steps for Maintaining the Privacy and Security of Patient Information" and "Your Mobile Device and HIPAA." Over 188,000 health care professionals took part in these training modules from 2013 through 2014.

- In 2013 and 2014, cohosted OCR's annual "Safeguarding Health Information: Building Assurance through HIPAA Security" conference with the National Institute for Standards and Technology. The two-day annual conference explores 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 launched a Digital Privacy Notice Challenge to leverage the model Notices of Privacy Practices (NPP): http://oncchallenges.ideascale.com/. Among other innovations, the challenge fostered the creation of a mobile, responsive digital version of the NPP which allows health care providers to offer an accessible web application of this required notice to their patients. The application works on any device with a web browser.

- In partnership with ONC, OCR developed a downloadable HIPAA Security Risk Assessment Tool to assist health care providers and other professionals as they perform a risk analysis as required under HIPAA: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool. The Tool is a self-contained, operating system (OS) independent application that can be run on various environments including desktop and laptop computers and Apple's iOS for iPad. The iOS Tool application for iPad is available at no cost, can be downloaded from Apple's App Store. The Security Risk Assessment Tool walks users through each HIPAA requirement, and presents corresponding questions to help self-measure an organization's compliance activities.

Plans for Future Increased Enforcement

Based on the HITECH Act's 2009 mandate, OCR plans to continue prioritizing resolution agreements as a means of increasing awareness in the HIPAA-regulated community about continuing issues with noncompliance with the HIPAA Rules. Specific areas on which OCR intends to focus include business associate compliance, compliance with the risk analysis and risk management requirements in the HIPAA Security Rule, breaches due to cyber security incidents, and individual rights under the HIPAA Privacy Rule.