Annual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance

For Calendar Years 2009 and 2010

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 to the Committee on Health, Education, Labor, and Pensions of the Senate, and to the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives regarding compliance with the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191). For the years for which the report is prepared, the report summarizes complaints received by the Department of alleged violations of the provisions of Subtitle D of the HITECH Act, as well as of the HIPAA Privacy and Security 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 web site of the Department. This report will be made available to the public at www.hhs.gov/ocr/privacy.

The HITECH Act requires that the report include, with respect to such complaints received during the year:

- 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[1] 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 review;
- the number of subpoenas 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] Corrective action includes activities that a covered entity takes as a result of technical assistance provided by OCR. Therefore, although OCR's data systems cannot generate concrete data on the numbers of entities that received technical assistance, our systems can generate the number of cases that resulted in the covered entity taking corrective action to address the Privacy or Security Rule violation. While OCR offered technical assistance to covered entities that were involved in cases resolved through corrective action, it was the corrective action that resulted in the covered entity making systemic changes necessary to ensure the privacy and security of the protected health information.

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 entities covered by HIPAA, defined in the HIPAA Privacy and Security Rules as "covered entities." 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 HIPAA Privacy Rule

The Department issued a final rule on December 28, 2000, which was amended in August 2002, addressing the privacy of individually identifiable health information. The HIPAA Privacy Rule, found at 45 CFR Part 160 and Subparts A and E of Part 164, provides important federal protections for individually identifiable health information held by covered entities (protected health information or "PHI") and gives individuals rights with respect to that information. Covered entities 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 Privacy Rule strikes a balance that protects the privacy of the health information of individuals while permitting important uses and disclosures of information, such as those for treatment of an individual and payment for health care, for certain public health purposes, in emergency situations, and to the friends and family involved in the care of an individual. The Privacy Rule also provides individuals with rights to be informed of a covered entity's privacy practices, obtain a copy of their medical records and certain other PHI, have incorrect or incomplete health information about them amended, and learn of certain disclosures of their PHI made by a covered entity or business associate, among other rights. The Secretary delegated the authority to administer and enforce the Privacy Rule to the Department's Office for Civil Rights (OCR) in December 2000.

The HIPAA Security Rule

As Subtitle F of HIPAA also required the Secretary to establish standards for the security of individually identifiable health information, the Department issued the Security Standards for the Protection of Electronic Protected Health Information, commonly known as the HIPAA Security Rule, on February 20, 2003. The 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 a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI. The Secretary initially delegated the authority to administer and enforce the Security Rule to the Centers for Medicare and Medicaid Services (CMS), and from 2003 to July 27, 2009, CMS administered the Security Rule. However, in recognition of the future increase in electronic PHI as a result of the adoption of electronic health records, and in recognition of the HITECH Act's provisions regarding privacy and security enforcement, the Secretary re-delegated the authority to administer and to enforce the Security Rule to OCR on July 27, 2009.

Enforcement Process

For most HIPAA covered entities, compliance with the Privacy Rule was required by April 14, 2003, and compliance with the Security Rule by April 20, 2005.

OCR enforces the Privacy and Security Rules by investigating written complaints filed with OCR, either on paper or electronically, by conducting compliance reviews to determine if covered entities are in compliance with the Rules, and by providing education and outreach to foster compliance with the Rules' requirements. 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 Privacy or Security Rules was required.

- The complaint must be filed against an entity that is required by law to comply with the Privacy and Security Rules.[2]

- A complaint must describe an activity that, if determined to have occurred, would violate the Privacy or Security Rule.

- Complaints must be filed within 180 days of when the individual submitting the complaint knew or should have known about the alleged violation of the Privacy or Security Rule. 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).

If OCR accepts a complaint for investigation, OCR will notify the individual who filed the complaint and the covered entity named in the complaint. Additionally, OCR may open compliance reviews of covered entities based on an event or incident that may implicate the Privacy and Security Rules, without reference to a complaint received from an individual. Further, OCR investigates the Privacy and Security Rule issues associated with all breach reports of breaches affecting 500 or more individuals. 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 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, OCR reviews the case for potential Privacy Rule and Security Rule issues and may investigate the case.

[2] The HITECH Act expanded liability for compliance with certain provisions of the Privacy and Security Rules to business associates of covered entities. The Department is currently undertaking a rulemaking to implement these provisions.

In some cases, OCR may determine, based on the evidence, that the covered entity did not violate the requirements of the Privacy or Security Rules. However, if the evidence indicates that the covered entity was not in compliance, under the current Enforcement Rule, OCR will first attempt to resolve the case informally with the covered entity by obtaining voluntary compliance through corrective action, which may include a resolution agreement.[3] In all such cases, OCR must obtain satisfactory documentation and other evidence from covered entities that the covered entities undertook the required corrective action to resolve the allegations. Most Privacy and Security Rule investigations are concluded to the satisfaction of OCR through these types of resolutions. However, if a covered entity refuses to take action to resolve the matter informally in a way that is satisfactory to OCR, OCR notifies the covered entity of a proposed determination of a violation of the Privacy and Security Rules for which OCR is seeking civil money penalties (CMPs). If CMPs are imposed, the covered entity may request a hearing in which a Departmental administrative law judge decides if the penalties are supported by the evidence in the case. OCR provides written notification to the individual who filed the complaint, if an investigation was initiated by a complaint, and to the covered entity of the resolution result. Through the end of calendar year 2010, OCR resolved all cases informally by obtaining voluntary compliance through corrective action from, which may include in certain cases resolution agreements with, covered entities.[4]

Enforcement Data

The following section provides an overview of the cumulative enforcement data through the end of calendar year 2010, followed by specific enforcement data for 2009 and 2010. As the Privacy and Security Rules were administered and enforced separately until July of 2009, we have continued to account for and to provide the enforcement data separately for each Rule.

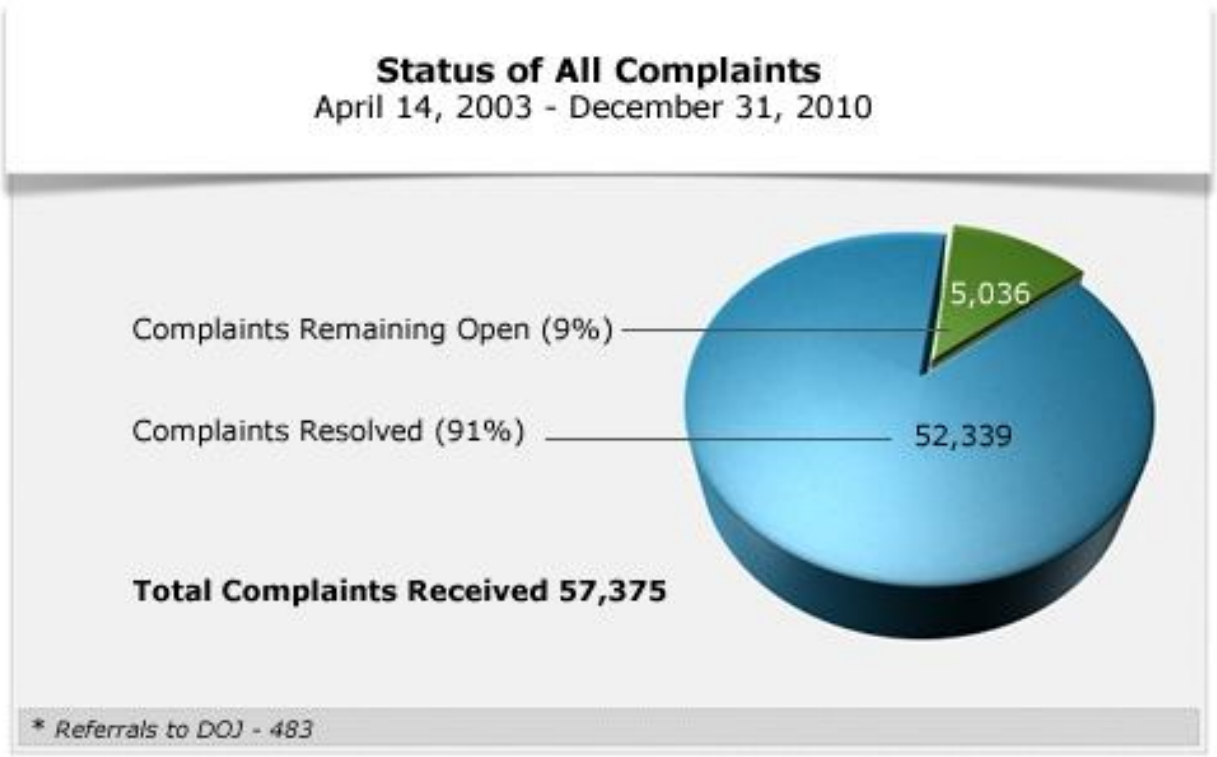
The Privacy Rule

Since 2003, OCR's Privacy Rule enforcement activities have obtained significant results that have improved the privacy practices of covered entities. The changes obtained by OCR in the privacy practices of covered entities, in turn, have improved the privacy protection of health information for individuals served by these covered entities.

[3] OCR proposed changes to these provisions of the HIPAA Enforcement Rule on July 14, 2010, which would provide the Secretary of the Department with the discretion to proceed directly to a civil money penalty in cases involving willful neglect on the part of a covered entity. OCR is currently working on a final rule to implement modifications to the HIPAA Enforcement Rule.

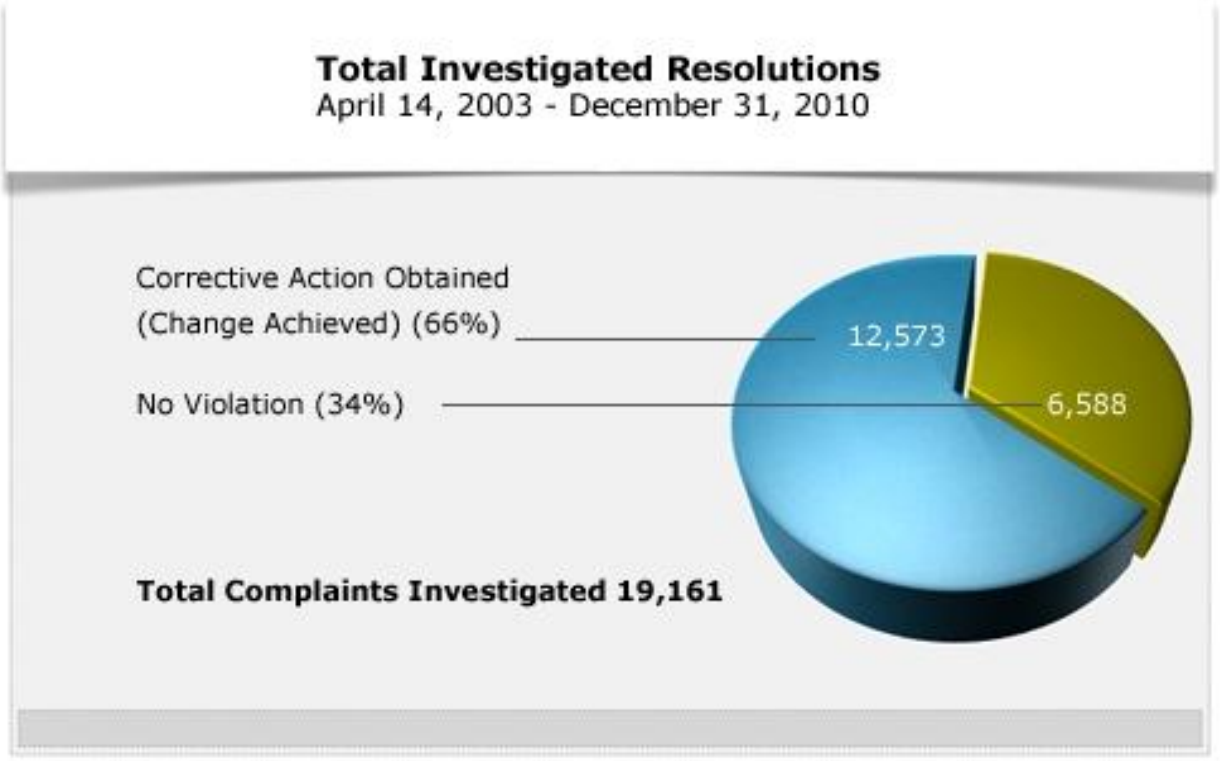
[4] All resolution agreements entered into by the Department prior to February 17, 2010, contain settlement amounts, which were paid to the General Treasury. Pursuant to the HITECH Act, after February 17, 2010, settlement amounts or CMPs, including the settlement amount paid by Rite Aid pursuant to its resolution agreement, are paid to and used by OCR for enhanced enforcement of the HIPAA Rules. Please see pages 18-19 of this report for additional details on the Rite Aid settlement. Note that on February 4, 2011, the Department imposed a CMP of $4.3 million on Cignet Health of Prince George's County, MD, for violation of the HIPAA Rules. This was the first CMP issued by the Department for violations of the HIPAA Rules. As this CMP was issued in 2011, it is not discussed in this report.

All Privacy Rule Complaints



From April 14, 2003, the compliance date of the Privacy Rule, to December 31, 2010, OCR received 57,375 complaints alleging violations of the Privacy Rule. OCR resolved 52,339, or ninety-one percent, of the complaints received.

Investigated Resolutions of Privacy Rule Complaints



OCR investigated 19,161 privacy cases from 2003 through 2010. OCR investigated and resolved 12,573 cases involving allegations of violations of the Privacy Rule by requiring covered entities to make changes to their privacy practices and to take other corrective actions. OCR has successfully enforced the Privacy Rule in all cases where its investigation indicated noncompliance by providing technical assistance to and requiring the covered entity to take corrective actions. Corrective actions taken by covered entities include: correcting any problems indicated by evidence in the investigation; training employees; sanctioning employees; revising policies and procedures; and mitigating any alleged harm. The goal of corrective actions is systemic change in the covered entity's policies and actions to ensure the proper protection of health information of individuals served by the entity. OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.

In another 6,588 cases, investigations by OCR found that no violation of the Privacy Rule occurred.

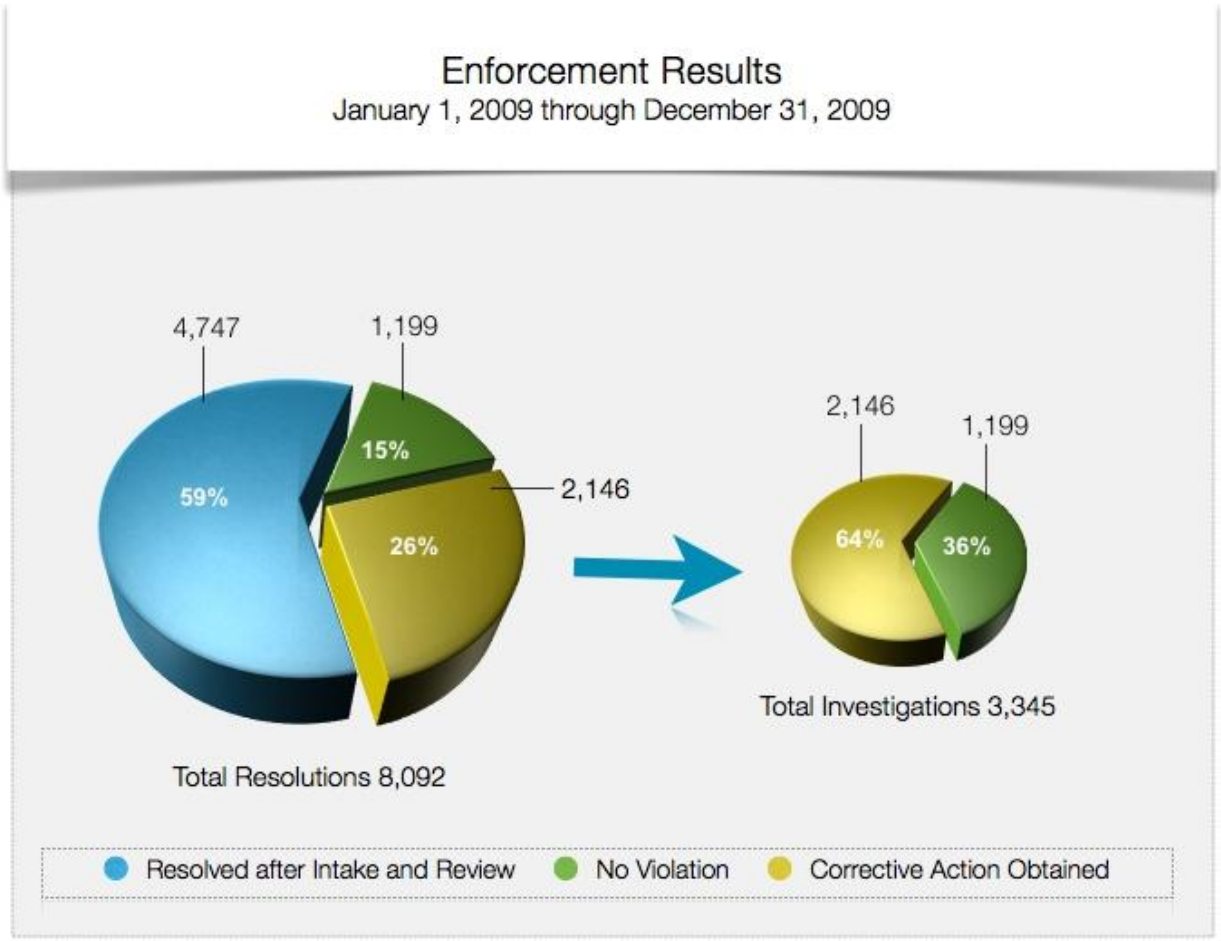
Other Privacy Rule Resolutions

OCR conducts compliance reviews of covered entities based on events or incidents that may implicate the Privacy and Security Rules, without reference to complaints received from individuals. During this time period, OCR opened 59 compliance reviews addressing allegations

of violations of the Privacy Rule that did not arise from complaints from individuals. OCR closed 43 of these compliance reviews.

In the remaining 33,178 resolved cases, OCR determined that the complaint did not present an eligible case for enforcement of the Privacy Rule. In these cases, OCR lacked jurisdiction under the Privacy Rule because the complaint alleged a violation prior to the compliance date, alleged a violation by an entity not covered by the Privacy Rule, was untimely or withdrawn, or because the activity described in the complaint did not violate the Privacy Rule. Finally, OCR made 483 referrals to DOJ.

2009 Privacy Rule Complaints



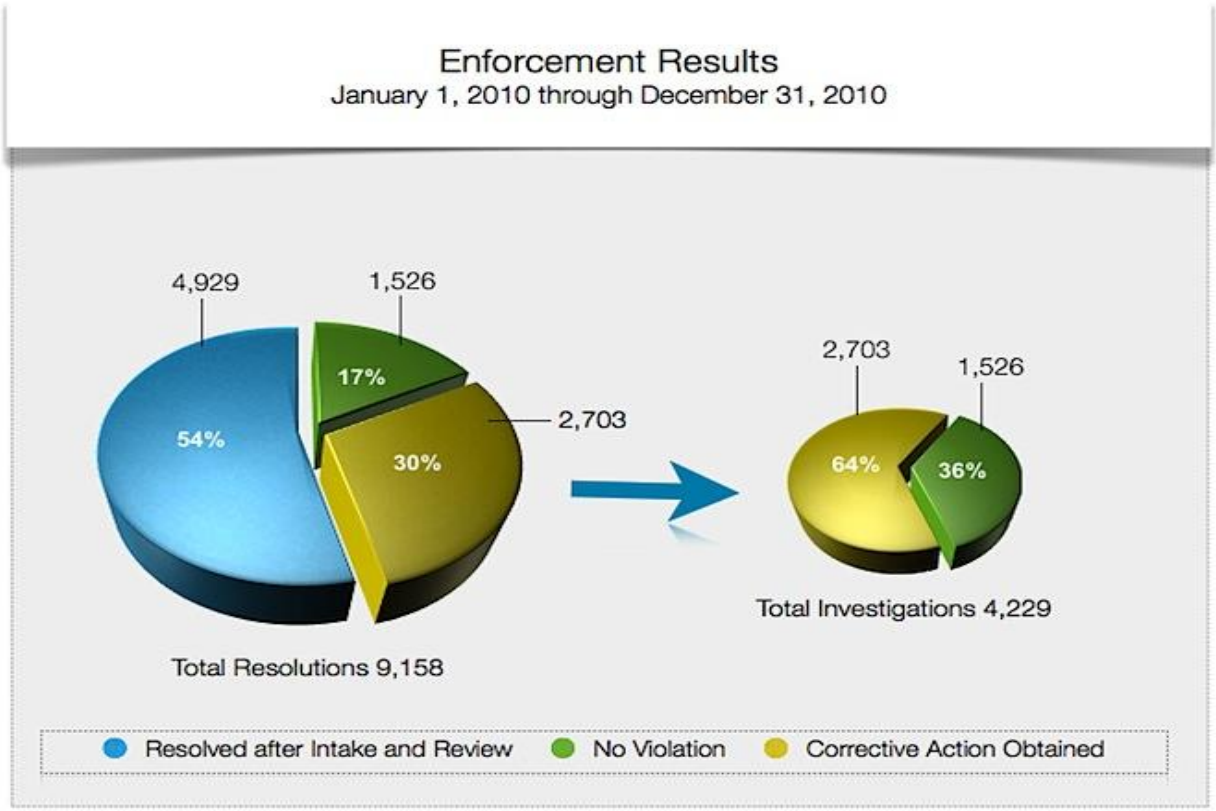
By the end of calendar year 2008, OCR resolved over eighty percent of the Privacy Rule complaints received, for a remainder of over 6,054 complaints that carried over into calendar year 2009. During calendar year 2009, OCR received an additional 7,567 complaints and resolved 8,092 complaints. In 2,146 complaints, OCR investigated the allegations of violations of the Privacy Rule, provided technical assistance to the covered entity, and required the covered entity to take corrective action. In 1,199 complaints, OCR investigated the allegations and found that no violation of the Privacy Rule had occurred. Finally, in 4,747 complaints, OCR

determined that it did not have jurisdiction under the Privacy Rule to investigate the allegations because the complaint alleged a violation prior to the compliance date, alleged a violation by an entity not covered by the Privacy Rule, was untimely or withdrawn, or because the activity described in the complaint did not violate the Privacy Rule.

2009 Privacy Rule Compliance Reviews

At the end of calendar year 2008, OCR had 27 open privacy compliance reviews.[5] During calendar year 2009, OCR opened an additional 16 privacy compliance reviews, and resolved 13 privacy compliance reviews. In all compliance reviews resolved in 2009, OCR obtained voluntary compliance through corrective action by the covered entity.

2010 Privacy Rule Complaints



During calendar year 2010, OCR received an additional 8,524 complaints and resolved 9,158 complaints. In 2,703 complaints, OCR investigated the allegations of violations of the Privacy Rule, provided technical assistance to the covered entity, and required the covered entity to take corrective action. In 1,526 complaints, OCR investigated the allegations and found that no violation of the Privacy Rule had occurred. Finally, in 4,929 complaints, OCR determined that it

[5] OCR may consolidate open Privacy Rule complaints and compliance reviews in certain circumstances, and may make other adjustments to the inventory of cases and compliance reviews, which may alter the number of compliance reviews remaining open at the end of a calendar year.

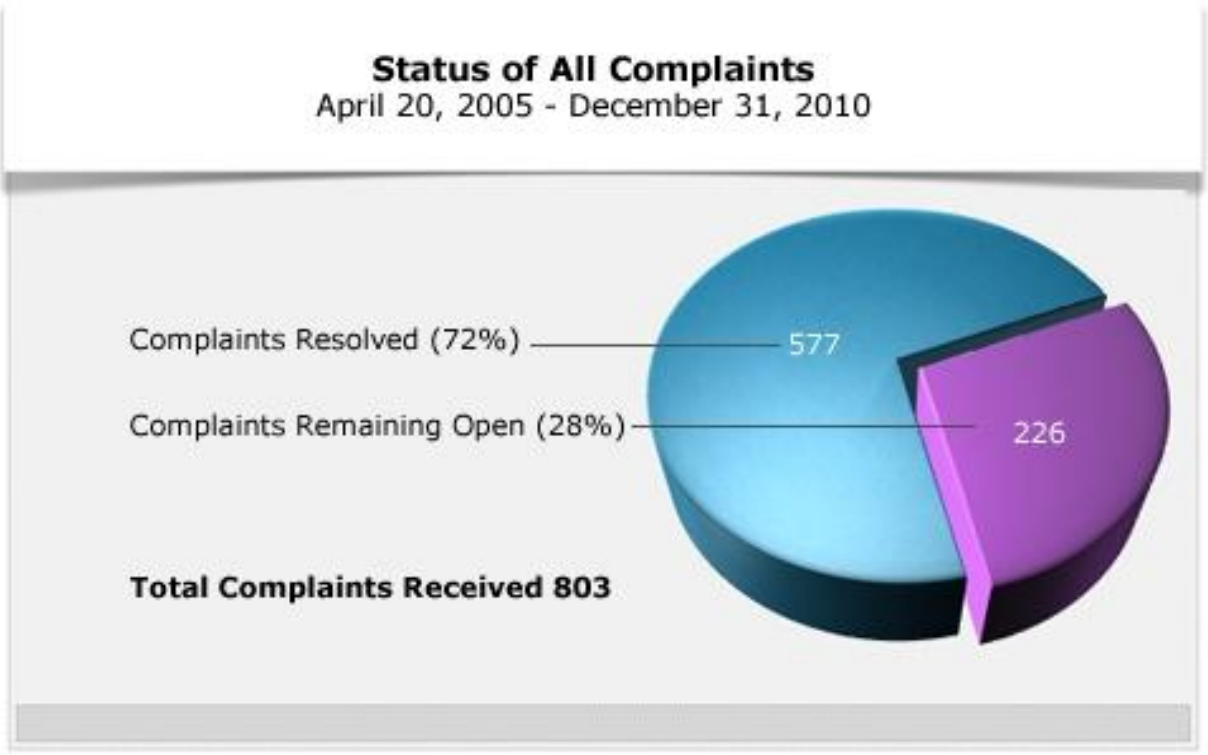
did not have jurisdiction under the Privacy Rule to investigate the allegations because the complaint alleged a violation prior to the compliance date, alleged a violation by an entity not covered by the Privacy Rule, was untimely or withdrawn, or because the activity described in the complaint did not violate the Privacy Rule.

2010 Privacy Rule Compliance Reviews

At the end of calendar year 2009, OCR had 24 open privacy compliance reviews.[6] During calendar year 2010, OCR opened an additional six privacy compliance reviews, and resolved 14 privacy compliance reviews. In all compliance reviews resolved in 2010, OCR obtained voluntary compliance through corrective action by the covered entity.

The Security Rule

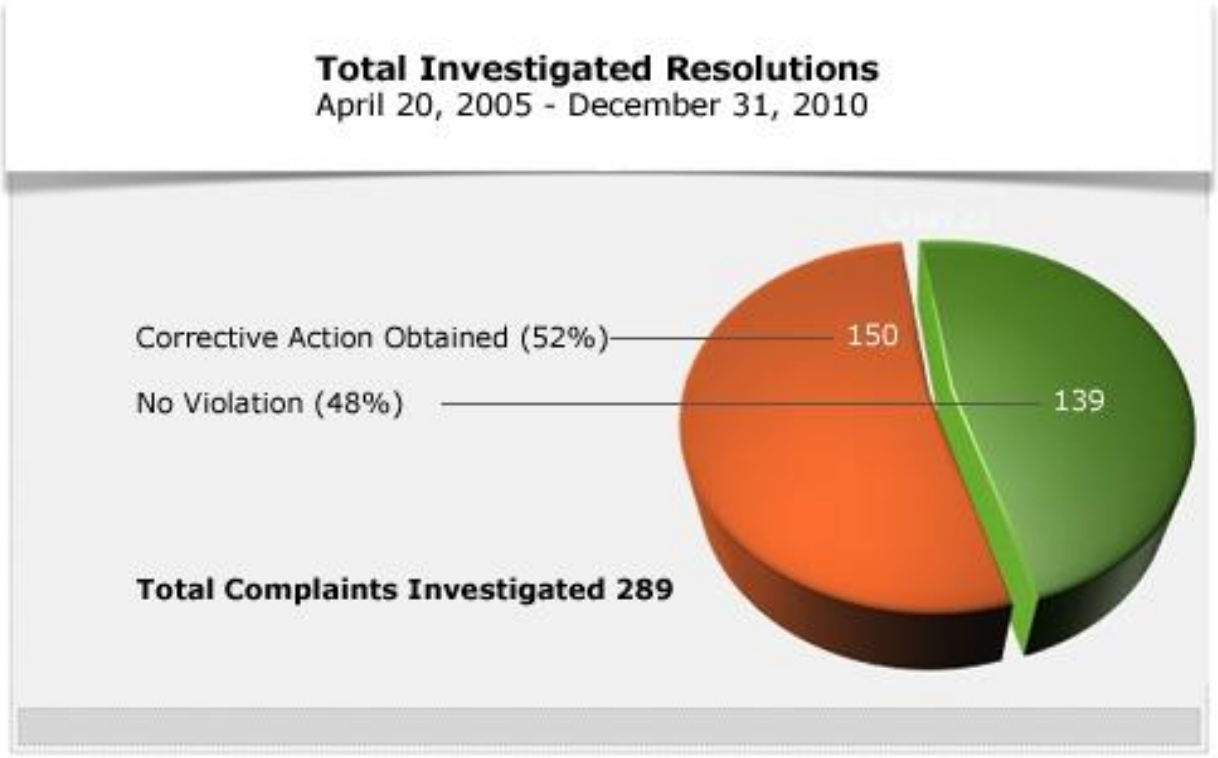
All Security Rule Complaints



From April 20, 2005, the compliance date of the HIPAA Security Rule, to December 31, 2010, OCR received 803 complaints alleging violations of the Security Rule. The Department resolved 577, or seventy-two percent, of the complaints received.

[6] OCR may consolidate open Privacy Rule complaints and compliance reviews in certain circumstances, and may make other adjustments to the inventory of cases and compliance reviews, which may alter the number of compliance reviews remaining open at the end of a calendar year.

Security Rule Investigated Resolutions



The Department investigated and resolved over 150 cases involving allegations of violations of the Security Rule by requiring changes in security practices and other corrective actions by covered entities. The Department has successfully enforced the Security Rule in all cases where an investigation indicated noncompliance by providing technical assistance to and requiring the covered entity to take corrective actions. Corrective actions taken by covered entities include: correcting any problems indicated by evidence in the investigation; training employees; sanctioning employees; revising policies and procedures; and mitigating any alleged harm. Corrective actions obtained by the Department from covered entities have improved the privacy protection of health information for individuals served by such covered entities. The Department has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.

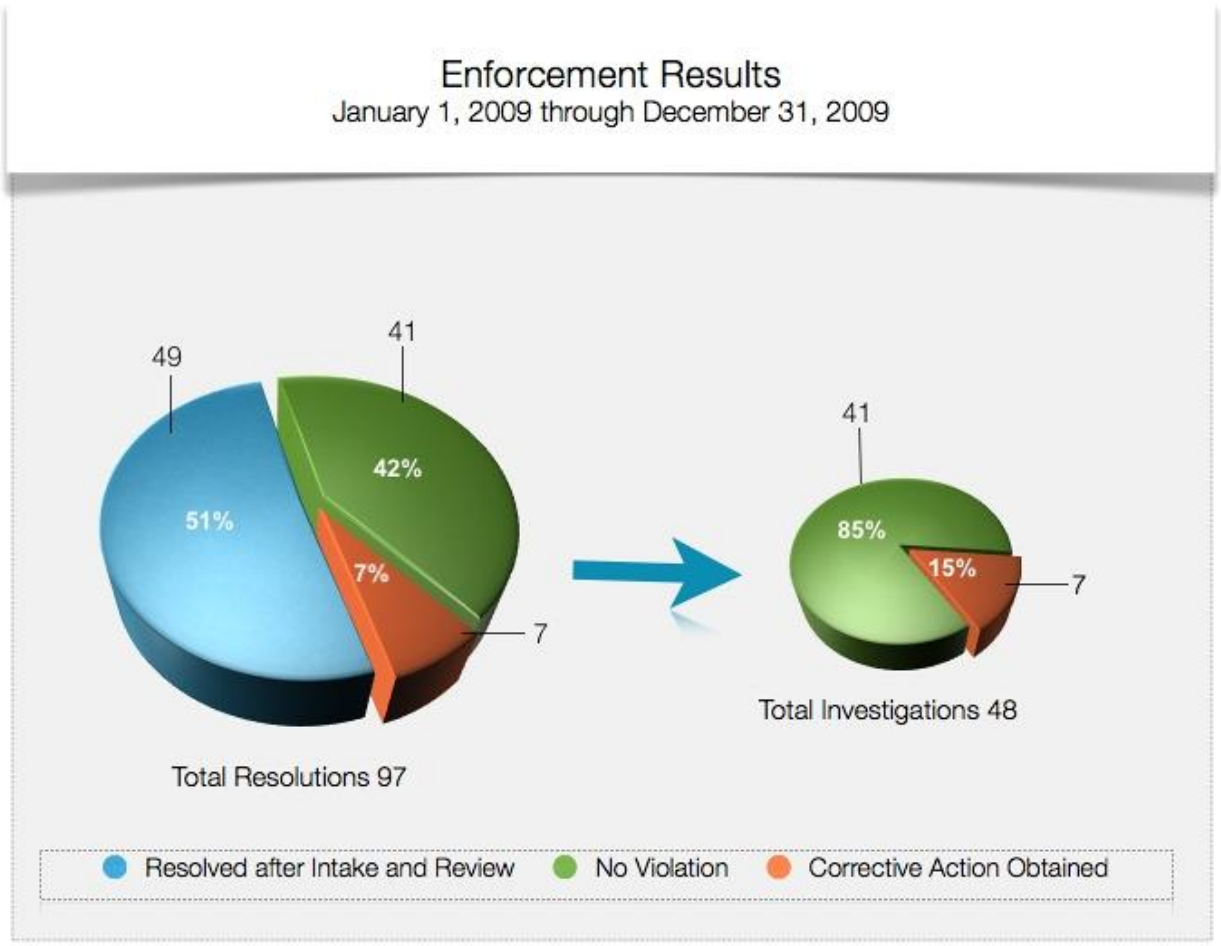
In another 139 cases, investigations by the Department found that no violation of the Security Rule occurred.

Other Security Rule Resolutions

In the remaining 288 resolved cases, the Department determined that the complaints did not present eligible cases for enforcement of either the Security Rule or the Privacy Rule. In these cases, the Department also lacked jurisdiction under the Rules, because the complaint alleged a violation prior to the compliance date, alleged a violation by an entity not covered by the Rules,

was untimely or withdrawn, or because the activity described in the complaint did not violate the Rules. Also during this time period, the Department opened 38 compliance reviews and closed 23 compliance reviews.

2009 Security Rule Complaints



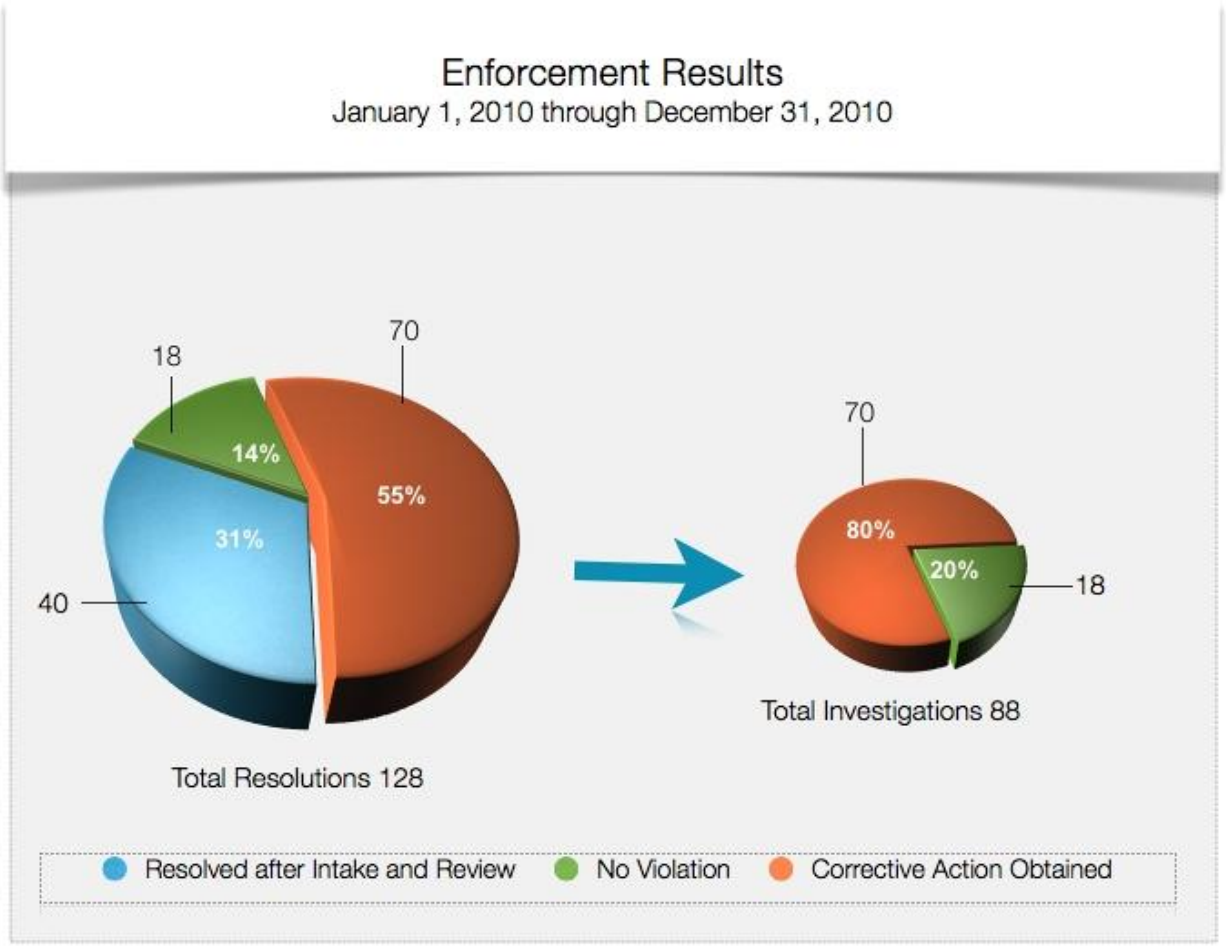
By the end of calendar year 2008, the Department resolved over seventy-nine percent of the Security Rule complaints received, for a remainder of over 95 complaints that carried over into calendar year 2009. During calendar year 2009, the Department received an additional 80 complaints and resolved 97 complaints. In seven complaints, the Department investigated the allegations of violations of the Security Rule, and provided technical assistance to the covered entity, and required the covered entity to take some corrective action. In 41 complaints, the Department investigated the allegations and found that no violation of the Security Rule occurred. Finally, in 49 complaints, the Department determined that it did not have jurisdiction under the Security Rule to investigate the allegations because the complaint alleged a violation prior to the compliance date, alleged a violation by an entity not covered by the Security Rule,

was untimely or withdrawn, or because the activity described in the complaint did not violate the Security Rule.

2009 Security Rule Compliance Reviews

At the end of calendar year 2008, the Department had 13 security compliance reviews that carried over into calendar year 2009. During calendar year 2009, the Department opened an additional eight security compliance reviews, and resolved four security compliance reviews. In all compliance reviews closed in 2009, the Department obtained voluntary compliance through corrective action by the covered entity.

2010 Security Rule Complaints



During calendar year 2010, OCR received an additional 243 complaints and resolved 128 complaints. In 70 complaints, OCR investigated the allegations of violations of the Security Rule, and provided technical assistance to the covered entity, and required the covered entity to take some corrective action. In 18 complaints, OCR investigated the allegations and found that no violation of the Security Rule occurred. Finally, in 40 complaints, OCR determined that it did

not have jurisdiction under the Security Rule to investigate the allegations because the complaint alleged a violation prior to the compliance date, the complaint alleged a violation by an entity not covered by the Security Rule, the complaint was untimely or withdrawn, or the activity described did not allege a violation of the Security Rule.

2010 Security Rule Compliance Reviews

At the end of calendar year 2009, OCR had 19 security compliance reviews that carried over into calendar year 2010.[7] During calendar year 2010, OCR resolved four security compliance reviews. In all compliance reviews closed in 2010, OCR obtained voluntary compliance through corrective action by the covered entity.

Issues and Entities

From the compliance date to December 31, 2010, the compliance issues investigated most by OCR with regard to the Privacy Rule, compiled cumulatively in order of frequency, are: impermissible uses and disclosures of PHI; lack of safeguards of PHI; denial of individuals' access to their PHI; uses or disclosures of more than the minimum necessary PHI; and the inability of individuals to file complaints with covered entities. From the compliance date to December 31, 2010, the compliance issues investigated most by OCR with regard to the Security Rule, compiled cumulatively in order of frequency, are failure to demonstrate adequate policies and procedures or safeguards to address: response and reporting of security incidents; security awareness and training; access controls; information access management; and workstation security.

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; health plans, which include group health plans and health insurance issuers; and pharmacies.[8]

Subpoenas, Case Examples, Resolution Agreements, and Audits

The following section provides information regarding subpoenas, case examples, resolution agreements, and audits in enforcement of both the Privacy Rule and the Security Rule during 2009 and 2010.

Subpoenas

On February 12, 2009, OCR issued a subpoena directing a covered entity to produce evidence required for an investigation of its compliance with the Privacy Rule. It was the first subpoena

[7] As with Privacy Rule cases, OCR may consolidate open Security Rule complaints and compliance reviews in certain circumstances, and may make other adjustments to the inventory of cases and compliance reviews, which may alter the number of compliance reviews remaining open at the end of a calendar year.

[8] Currently, the Department's information systems do not capture the types of entities required to take corrective action to achieve voluntary compliance with regard to the Security Rule. OCR intends to capture this information in the near future with updated information systems.

issued by OCR pursuant to its subpoena authority under HIPAA (42 U.S.C. 1320d-5, 1320a-7a(j)). OCR's investigation of a physician practice sought to establish whether the practice had provided an individual with a copy of her medical records as required by the Privacy Rule at 45 CFR 164.524. The subpoena sought copies of the individual's medical records and the entity's policies on the medical record access requirement. On March 17, 2009, the covered entity responded to the subpoena by partially producing the requested documents. On May 12, 2009, the covered entity produced the remaining requested documents. OCR closed the case based on the covered entity's voluntary compliance on May 18, 2009.

On June 26, 2009, OCR issued a subpoena directing a covered entity to produce evidence required for an investigation of its compliance with the Privacy Rule. It was the second subpoena issued by OCR pursuant to its subpoena authority under HIPAA (42 U.S.C. 1320d-5, 1320a-7a(j)). OCR's investigation of a large physician practice sought to establish whether the practice had provided 16 requesting individuals with copies of their medical records as required by the Privacy Rule at 45 CFR 164.524. The subpoena sought copies of the individuals' medical records and the entity's policies on the medical record access requirement. The covered entity did not respond to the subpoena. On February 2, 2010, OCR, represented by DOJ, filed a petition to enforce the subpoena in the United States District Court (MD). On April 7, 2010, the covered entity produced the records.[9]

Case Examples

The following examples are summaries of actual Privacy and Security Rule cases investigated and resolved by the Department in 2009 and 2010.

- An individual filed a complaint with OCR alleging that a private practice physician denied her access to her medical records because she had an outstanding balance for services the physician had provided. During OCR's investigation, the physician confirmed that the individual was not given access to her medical record because of the outstanding balance. OCR provided technical assistance to the physician, explaining that, in general, the Privacy Rule requires that a covered entity provide an individual with access to her medical record within 30 days of a request, regardless of whether or not the individual has a balance due. Once the physician learned that he could not withhold access until payment was made, the physician provided the complainant a copy of her medical record.

- An individual who was both a patient and an employee of the hospital filed a complaint with OCR alleging that her PHI was impermissibly disclosed to her supervisor. OCR's investigation revealed that the hospital distributed an Operating Room (OR) schedule to employees via e-mail; this OR schedule contained information about the individual's upcoming surgery. While the Privacy Rule may permit the disclosure of an OR schedule containing PHI, in this case, a hospital employee shared the OR schedule with the individual's supervisor, who was not part of the employee's treatment team, and did not

[9] This subpoena was issued in conjunction with the investigation against Cignet Health of Prince George's County, MD, in which case the Department also imposed the first civil money penalty for violations of the HIPAA Privacy Rule. As this CMP was issued in 2011, it is not discussed in this report.

need the information for payment, health care operations, or other permissible purposes. The hospital disciplined and retrained the employee who made the impermissible disclosure. Additionally, in order to prevent similar incidents, the hospital undertook a complete review of the distribution of the OR schedule. As a result of this review, the hospital revised the distribution of the OR schedule, limiting it to those who have "a need to know."

- A physician practice requested that patients sign an agreement entitled "Consent and Mutual Agreement to Maintain Privacy." The agreement prohibited the patient from directly or indirectly publishing or airing commentary about the physician, his expertise, and/or treatment in exchange for the physician's compliance with the Privacy Rule. A patient's rights under the Privacy Rule are not contingent on the patient's agreement with a covered entity. A covered entity's obligation to comply with all requirements of the Privacy Rule cannot be conditioned on the patient's silence. OCR required the covered entity to cease using the patient agreement that conditioned the entity's compliance with the Privacy Rule. Additionally, OCR required the covered entity to revise its Notice of Privacy Practices.

- Media reports indicated that computer backup tapes containing electronic PHI for two million individuals were stolen from a vehicle used by a hospital's off-site storage vendor. OCR investigated the surrounding circumstances and subsequently instituted a compliance review to evaluate the hospital's overall compliance with the Security Rule. The compliance review revealed gaps in the hospital's Security Rule compliance program. As a result of the review, the hospital developed a corrective action plan, which included: the adoption of encryption technologies on all backup tapes that contained electronic PHI; termination of the off-site storage contract and reevaluation of contactor requirements to transport and store backup tapes; improvements to security awareness training policies; and revision of the process for periodic review and updates of policies and procedures.

- An individual filed a complaint with OCR after receiving a letter from a health care clinic reporting the theft of a computer that held PHI. OCR's investigation determined that the computer had been stolen while a reception desk was left unattended and that the electronic PHI on the computer's hard drive was not encrypted. OCR's investigation revealed that, following the theft, the covered entity took corrective actions to improve its physical security safeguards and prevent similar unauthorized disclosures from occurring in the future. The entity retrained its employees on privacy and security policies and procedures, encrypted its computers and electronic devices, installed locking mechanisms, and instituted a policy of closing and locking doors when offices were unattended.

- An individual filed a complaint with OCR alleging that the PHI of health plan members was available on the internet through online searches. OCR's investigation of the complaint revealed gaps in the covered entity's Security Rule compliance program. Specifically, the entity implemented system changes to its web servers without analyzing the associated risks, and without performing an evaluation of how well its security

measures responded to the changes, as required by the Security Rule. As a result, the entity was unaware that unsecured member information was exposed on the internet and did not take actions to evaluate and revise its practices until several months later, when it was notified of the impermissible disclosure. At the conclusion of the investigation, OCR obtained assurances from the entity that it had initiated evaluations of its existing security measures and modifications of its policies, procedures, and system designs to secure its members' PHI.

- An individual filed a complaint with OCR alleging that a mental health center (the "Center") refused to provide her with a copy of her medical record, including psychotherapy notes. OCR's investigation revealed that the Center provided the complainant with an opportunity to review her medical record, including the psychotherapy notes, with her therapist, but the Center did not provide her with a copy of her records. The Privacy Rule requires covered entities to provide individuals with access to their medical records; however, the Privacy Rule exempts psychotherapy notes from this requirement. Although the Center gave the complainant the opportunity to review her medical record, this did not negate the Center's obligation to provide the complainant with a copy of her records. Among other corrective action taken, the Center provided the complainant with a copy of her medical record and revised its policies and procedures to ensure that it provides timely access to all individuals.

- A private practice physician who was the principal investigator of a clinical research study disclosed a list of patients and diagnostic codes to a contract research organization to telephone patients for recruitment purposes. The disclosure was not consistent with documents approved by the Institutional Review Board (IRB). The private practice maintained that the disclosure to the contract research organization was permissible as a review preparatory to research. Activities considered "preparatory to research" include: preparing a research protocol; developing a research hypothesis; and identifying prospective research participants. Further, a researcher may not remove PHI from the covered entity. To remedy this situation, the private practice revised its policies and procedures regarding the disclosure of PHI and trained all physicians and staff members on the new policies and procedures. Under the revised policies and procedures, the practice may disclose PHI to an outside researcher for research recruitment, only if a valid authorization is obtained from each individual or if the covered entity obtains documentation that an alteration to or a waiver of the authorization requirement has been approved by an IRB or a Privacy Board.

Resolution Agreements[10]

[10]The Department entered into Resolution Agreements with Seattle-based Providence Health & Services (Providence) on July 16, 2008, with CVS Pharmacy, Inc. (CVS) on January 16, 2009, with Rite Aid Corporation on July 27, 2010, and with Management Services Organization Washington, Inc. on December 13, 2010, to settle potential violations of the Privacy and Security Rules. Providence agreed to pay $100,000 as a monetary settlement and to implement a detailed corrective action plan to ensure the appropriate safeguarding of electronic PHI against theft or loss, specifically relating to Providence's loss of electronic backup media and laptop computers containing electronic PHI in 2005 and 2006. As this agreement was signed in 2008, it is not included in this section.

Resolution Agreement with CVS Pharmacy, Inc.

On January 16, 2009, the Department reached agreement with CVS Pharmacy, Inc. (CVS) to settle potential violations of the Privacy Rule. To resolve OCR's investigation of its privacy practices, CVS agreed to pay $2.25 million and to implement a detailed Corrective Action Plan to ensure that its workforce members appropriately dispose of PHI, such as labels from prescription bottles and old prescriptions. The new practices apply to all of CVS's more than 6,300 retail pharmacies. In a coordinated action, CVS Caremark Corporation, the parent company of the pharmacy chain, also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the Federal Trade Commission Act.

CVS is the largest pharmacy chain in the country. OCR opened its investigation of CVS pharmacy compliance with the Privacy Rule after media reports alleged that PHI maintained by several retail pharmacy chains was being disposed of in dumpsters that were not secure and could be accessed by the public. At the same time, the FTC opened its investigation of CVS. OCR and the FTC conducted their investigations collaboratively. This is the first instance in which OCR has coordinated investigation and resolution of a matter with the FTC.

The Privacy Rule requires covered entities, including pharmacies, to safeguard the privacy of PHI, including such information during its disposal. Among other issues, OCR's investigation indicated that CVS failed to implement adequate policies and procedures to reasonably and appropriately safeguard PHI during the disposal process. OCR's investigation also indicated that CVS failed to adequately train employees on how to dispose of such information properly and did not maintain and implement a sanctions policy for members of its workforce who failed to comply with its disposal policies and procedures.

Under the Resolution Agreement, CVS agreed to pay a $2,250,000 resolution amount and implement a strong Corrective Action Plan that requires:

- revising and distributing its policies and procedures regarding disposal of PHI;
- sanctioning workers who do not follow them;
- training workforce members on these new requirements;
- conducting internal monitoring;
- engaging a qualified, independent third-party assessor to conduct assessments of CVS compliance with the requirements of the Corrective Action Plan for a period of three years and to render periodic reports to the Department;
- new internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures; and
- submitting compliance reports to the Department for a period of three years.

Both the Department and the FTC require CVS to actively monitor its compliance with the Resolution Agreement and FTC Consent Order.

Resolution Agreement with Rite Aid Corporation

On July 27, 2010, the Department reached agreement with Rite Aid Corporation and its 40 affiliated entities (Rite Aid) to settle potential violations of the Privacy Rule. To resolve OCR's investigation of its privacy practices, Rite Aid Corporation agreed to pay $1 million to settle potential violations of the Privacy Rule. In a coordinated action, Rite Aid also signed a consent order with the FTC to settle potential violations of the FTC Act.

Rite Aid, one of the nation's largest drug store chains, also agreed to take corrective action to improve policies and procedures to safeguard the privacy of its customers when disposing of identifying information on pill bottle labels and other health information. The settlements apply to all of Rite Aid's nearly 4,800 retail pharmacies and follow an extensive joint investigation by OCR and the FTC.

OCR opened its investigation of Rite Aid after television media videotaped incidents in which pharmacies were shown to have disposed of prescriptions and labeled pill bottles containing individuals' identifiable information in industrial trash containers that were accessible to the public. These incidents were reported as occurring in a variety of cities across the United States. Rite Aid pharmacy stores in several of the cities were highlighted in media reports.

Among other issues, the reviews by OCR and the FTC indicated that Rite Aid:

- failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process;
- failed to adequately train employees on how to dispose of such information properly; and
- did not maintain a sanctions policy for members of its workforce who failed to properly dispose of patient information.

Under the Resolution Agreement, Rite Aid agreed to pay a $1 million resolution amount and implement a strong Corrective Action Plan that includes:

- revising and distributing its policies and procedures regarding disposal of protected health information and sanctioning workers who do not follow them;
- training workforce members on these new requirements;
- conducting internal monitoring; and
- engaging a qualified, independent third-party assessor to conduct compliance reviews and render reports to OCR.

Rite Aid also agreed to external independent assessments of its pharmacy stores' compliance with the FTC consent order. The OCR Corrective Action Plan is in place for three years; the FTC order is in place for 20 years.

Resolution Agreement with Management Services Organization Washington, Inc.

On December 13, 2010, the Department reached agreement with Management Services Organization Washington, Inc. (MSO), to settle potential violations of the HIPAA Privacy and Security Rules. This settlement arose from and was made in coordination with the HHS Office of the Inspector General and the U.S. Department of Justice, which had been investigating MSO for violations of the Federal False Claims Act.

In the agreement, MSO agreed to pay $35,000 and implement a detailed Corrective Action Plan to ensure that it will appropriately safeguard identifiable electronic patient information against impermissible use or disclosure. The Corrective Action Plan includes requirements for MSO to develop, maintain, and revise its policies and procedures and to appropriately train its workforce on these policies and procedures. OCR is monitoring MSO's compliance with the terms of the Corrective Action Plan and the Privacy and Security Rules for a period of two years.

The Resolution Agreement and Corrective Action Plan relate to MSO's disclosure of electronic protected health information to Washington Practice Management, LLC, owned by MSO, which used the information for marketing purposes. The OCR investigation showed that MSO intentionally did not have in place or implement appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of the protected health information.

Audits

Section 13411 of the HITECH Act, which became effective on February 17, 2010, authorizes the Department to provide for periodic audits to ensure that covered entities and business associates comply with the HIPAA Privacy and Security Rules. Generally, audits, unlike complaint investigations or compliance reviews, are reviews of covered entities and business associates that are initiated not because of any particular incident indicating noncompliance on the part of the covered entity or business associate, but rather based on application of a set of objective selection criteria. With the use of ARRA funds beginning in 2009, OCR initiated a study to determine the most effective means of implementing an audit program. The report from the study provided recommendations of several alternative program models. Based on OCR's assessment of the suggested audit models and with the support of ARRA funds, OCR has begun to develop a pilot audit program and a process for evaluating the effectiveness of the audit model selected.

Plans for Future Improved Enforcement

The Privacy and Security Rules give individuals rights over their health information, set rules and limits on the uses and disclosures of such health information by covered entities and their business associates, and create a foundation for consumer trust in health information technology. The Privacy Rule applies to all forms of individuals' PHI, whether electronic, written, or oral.

Additionally, the Security Rule requires entities covered by HIPAA to ensure that electronic PHI is secure. Such protections are essential in an increasingly electronic health care environment.

To improve enforcement of the HIPAA Privacy and Security Rules and to comply with the HITECH Act, OCR has issued an interim final rule (74 FR 56123) implementing many of the enforcement provisions of the HITECH Act that went into effect on February 18, 2009. These provisions provide for new enforcement categories based on culpability and for new penalties under the Privacy and Security Rules. The new civil money penalty amounts apply to Privacy and Security Rule violations occurring after February 17, 2009. As such, OCR will continue to work to identify complaints, to structure investigations pursuant to the new enforcement categories, and to pursue civil money penalties and monetary settlements in accordance with such categories.

OCR is also in the process of implementing the additional enforcement provisions of the HITECH Act, as well as many important privacy and security provisions, through notice and comment rulemaking, as required by the Administrative Procedure Act. These provisions include: business associate liability; new limitations on the sale of PHI, marketing, and fundraising communications; and stronger individual rights to access electronic medical records and restrict the disclosure of certain information. OCR published a Notice of Proposed Rulemaking (NPRM) on July 14, 2010 (75 FR 40868), addressing these provisions. The NPRM provides, as will the final rule that follows, specific information regarding the expected date of compliance and enforcement of these new requirements.

OCR will continue to work diligently to enforce both the current protections under the Privacy and Security Rules and the new protections provided by the HITECH Act, especially by leveraging state and federal partnerships including those OCR has already established with other federal agencies, such as DOJ and FTC. Additionally, as section 13410(e) of the HITECH Act provides for enforcement of HIPAA protections by state attorneys general, OCR will work closely with state attorneys general in the future. Further, to assist state attorneys general in their efforts to exercise their new enforcement authority and to promote productive and effective enforcement relationships with them, OCR conducted a series of training seminars focused on enforcement of the Privacy and Security Rules and continues to work with and develop training for the state attorneys general.

Finally, based on OCR's assessment of various audit models, OCR is proceeding to implement a pilot audit program and a process to evaluate the chosen audit model. First, OCR has contracted for the development of a database to enable the meaningful and objective selection of covered entities to be audited by OCR based on a variety of potential factors, including the types, sizes, and geographic locations of covered entities.

Second, OCR has contracted for the development of a compendium of compliance audit protocols for distinct types of covered entities and will use the protocols to conduct audits of up to 145 entities. The protocols will be a comprehensive methodology, serving as a single source of audit criteria, assessment methods, and procedures for conducting HIPAA Privacy and Security Rule and HITECH Breach Notification Rule compliance audits, reflecting the specific requirements that apply to each of the three types of covered entities: covered health care

providers, health plans and health care clearinghouses. Revisions and improvements to the audit protocols will be made throughout the pilot period to ensure the final protocols are effective, accurate, and objectively neutral instruments for the measurement of compliance across covered entities. OCR anticipates that all of the audits will be completed by December 31, 2012.

Finally, OCR is contracting for evaluation of the suitability and accuracy of the audit protocols used and the findings of the audits from the pilot program.