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

For Calendar Years 2011 and 2012

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[2] 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;

[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.

[2] In its resolution of complaints, OCR may provide covered entities and business associates with technical assistance and/or require them to undertake corrective action. For purposes of this report, the numbers of cases for which OCR provided technical assistance are combined with the numbers of cases in which OCR required corrective action into one category of investigated cases, because cases resolved with technical assistance prior to 2012 often involved significant investigatory work and coordination with the particular covered entity in the case. For future reports, technical assistance without corrective action will not be included in investigated cases, because such technical assistance no longer involves investigatory work that includes coordination with the covered entity or business associate.

- 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.

This report is prepared for calendar years 2011 and 2012. The Report to Congress on Compliance with the HIPAA Privacy and Security Rules for calendar years 2009 and 2010 is 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, expanded applicability of certain provisions of the HIPAA Rules to business associates of covered entities.[3] 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).

[3] On January 25, 2013, the Department published a final rule that implemented changes required by the HITECH Act and by the Genetic Information Nondiscrimination Act of 2008. 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. As business associates were not required to comply with these provisions of the HIPAA Privacy and Security Rules until September 23, 2013, the enforcement activity described in this report contains information pertaining to HIPAA covered entities only. Future reports will include information about enforcement against business associates.

The HIPAA Breach Notification Rule, found at 45 CFR Part 160 and Subparts A and D of Part 164, requires HIPAA covered entities to notify affected individuals, the Department, and in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates are also required to notify covered entities following the discovery of a breach.

For most HIPAA covered entities, compliance with the Privacy Rule was required by April 14, 2003, compliance with the Security Rule was required by April 20, 2005, and compliance with the Breach Notification Rule was required for breaches that occurred on or after September 23, 2009.[4] This report includes information about the Department's enforcement process with regard to the Privacy, Security, and Breach Notification Rules, 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 2011 and 2012. Additionally, the report includes a discussion of the Department's plans to improve enforcement of the Rules in 2013 and beyond.

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 of covered entities,[5] 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.

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

- Complaints must be filed within 180 days of when the individual submitting the complaint knew or should have known about the act or omission that is the subject of the complaint. OCR may waive this time limit if it determines that the individual submitting the complaint shows good cause for not submitting the complaint within the 180 day time

[4] 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.

[5] 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, during 2010, 2011, and 2012, OCR undertook several initiatives towards the establishment of an audit program.

frame (e.g., circumstances that made submitting the complaint within 180 days impossible).

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 explaining the results of the investigation to the parties involved.

If the evidence indicates that the covered entity or business associate was not in compliance, OCR will generally first attempt to resolve the case informally with the covered entity or business associate by obtaining voluntary compliance through corrective action, which may include a resolution agreement. However, OCR has the discretion to proceed directly to a civil money penalty (CMP) in an appropriate case, such as one involving particularly egregious circumstances.

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 CMPs 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, and, 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.

Finally, 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 2012, out of all the cases OCR attempted to resolve informally through a resolution agreement, only one case resulted in the imposition of a CMP.[6]

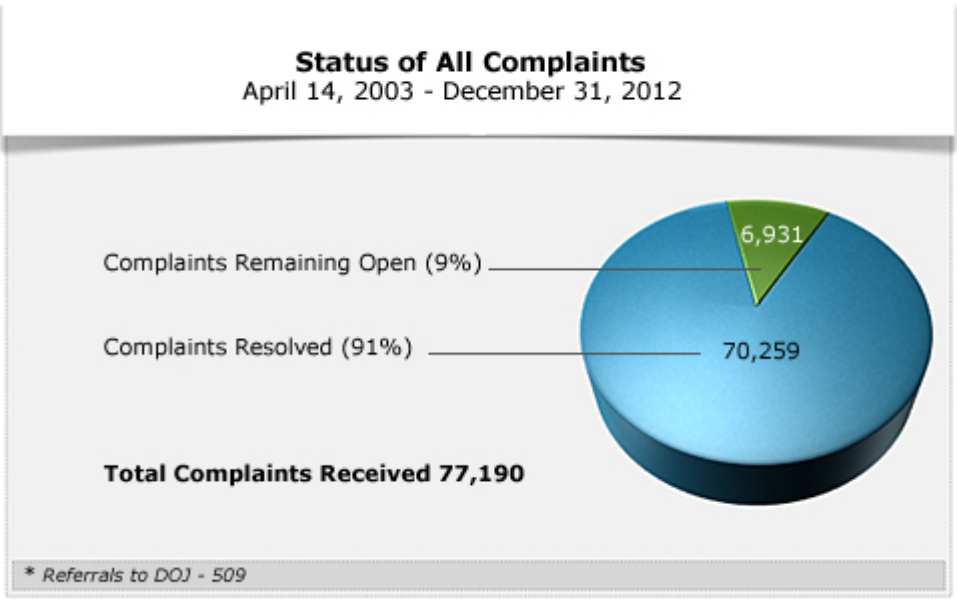
Enforcement Data

The following section provides an overview of the cumulative enforcement data through the end of calendar year 2012, followed by specific enforcement data for calendar years 2011 and 2012. Until 2010, complaints alleging violations of the HIPAA Security Rule were counted separately, as outlined in the Report to Congress on Compliance with the HIPAA Privacy and Security Rules for calendar years 2009 and 2010. In this report, complaints alleging violations of the HIPAA Security Rule are included in the general enforcement numbers.

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, 2012, OCR received 77,190 complaints alleging violations of the HIPAA Rules. As of December 31, 2012, OCR resolved 70,259, or ninety-one percent, of the complaints received. The majority of complaints received are resolved within one year of their receipt.

[6] 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 42,793 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, or described an activity that did not violate the HIPAA Rules.

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 2012, OCR investigated 27,466 complaints. Of those, OCR resolved 18,559 cases by requiring covered entities to take corrective actions and/or provided technical assistance to covered entities to resolve indications of noncompliance. Corrective actions taken by covered entities 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 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. Specific information about the major cases involving resolution agreements and the one case involving a CMP where informal resolution could not be achieved, follows below. Finally, in the other 8,907 cases investigated, OCR found that no violation of the HIPAA Rules occurred.

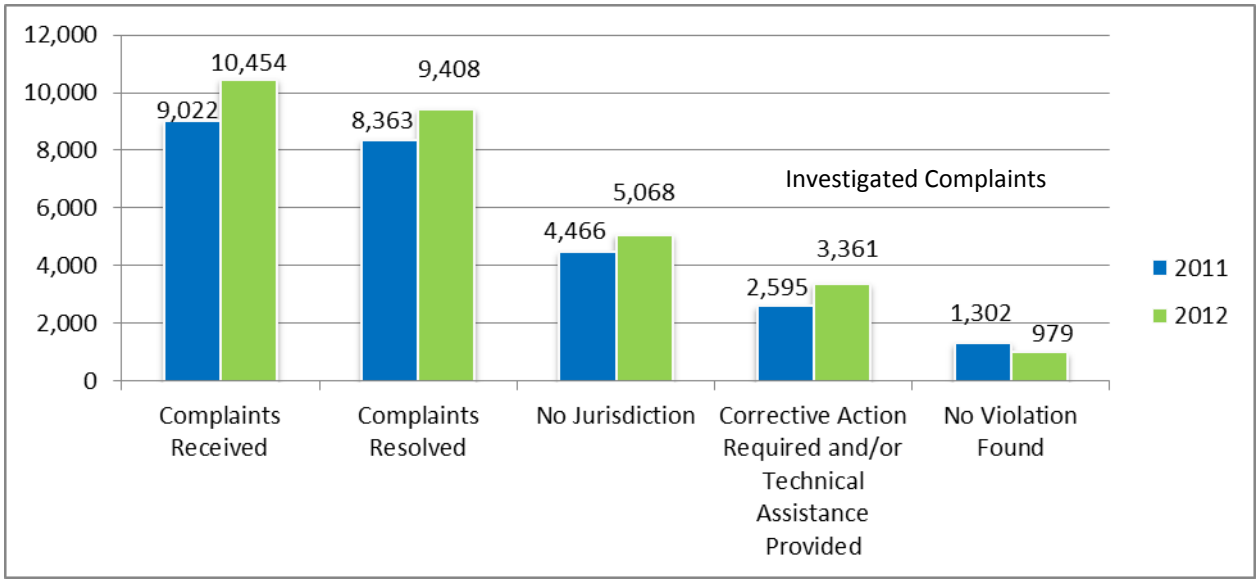
Compliance Reviews

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 2012, OCR opened at least 804 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 710 compliance reviews were opened as a result of a breach report affecting 500 or more individuals.

Issues and Entities

From 2003 to 2012, the compliance issues investigated most by OCR, 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 lack of administrative safeguards of ePHI. 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.

2011 and 2012 Complaints and Compliance Reviews



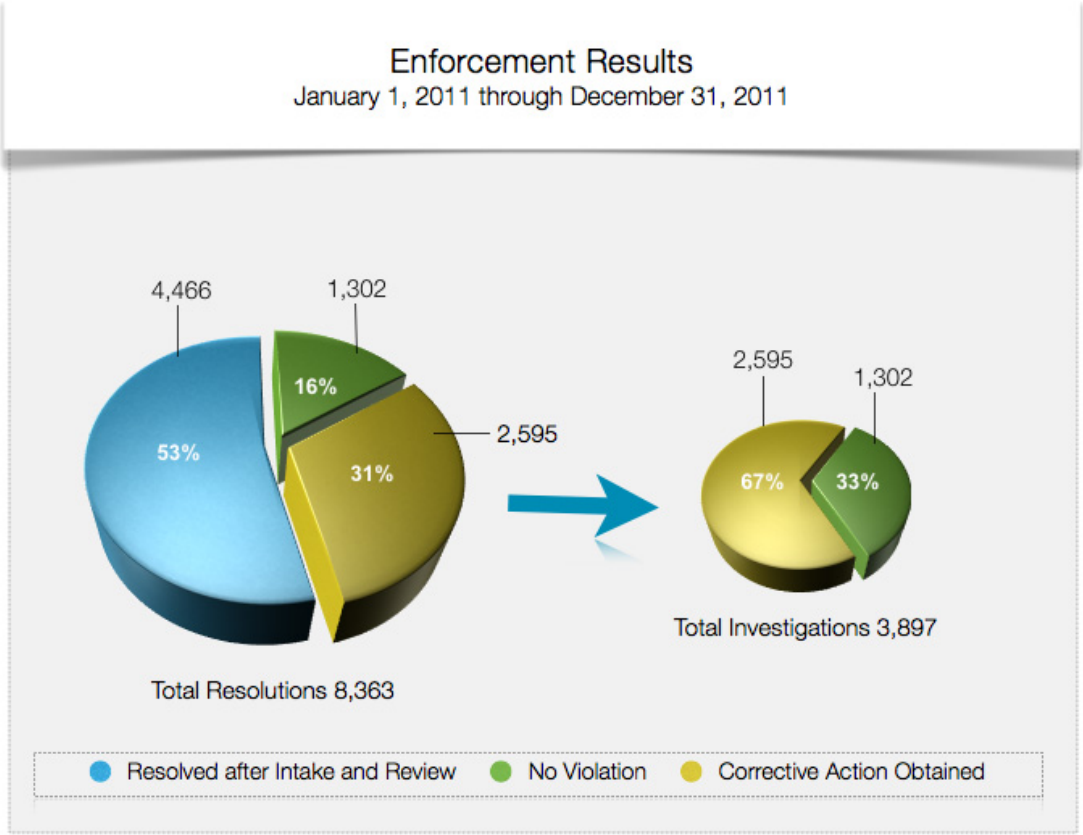
2011 Complaints and Compliance Reviews

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 2010, a remainder of approximately[7] 5,324 open complaints carried over into calendar year 2011. During calendar year 2011, OCR received an additional 9,022 complaints, representing the largest number of complaints received in any calendar year to that point, and an increase of 258 complaints from 2010. OCR resolved a total of 8,363 complaints in 2011.

In 2,595 of the complaints investigated in 2011, OCR provided technical assistance to the covered entity, and/or required the covered entity to take corrective action. In 1,302 of the complaints investigated, OCR found that no violation of the HIPAA Rules had occurred. Finally, in 4,466 complaints, 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] 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 2011, OCR opened at least 245 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 236 reviews were opened as a result of a breach report affecting 500 or more individuals.[8]



2012 Complaints and Compliance Reviews

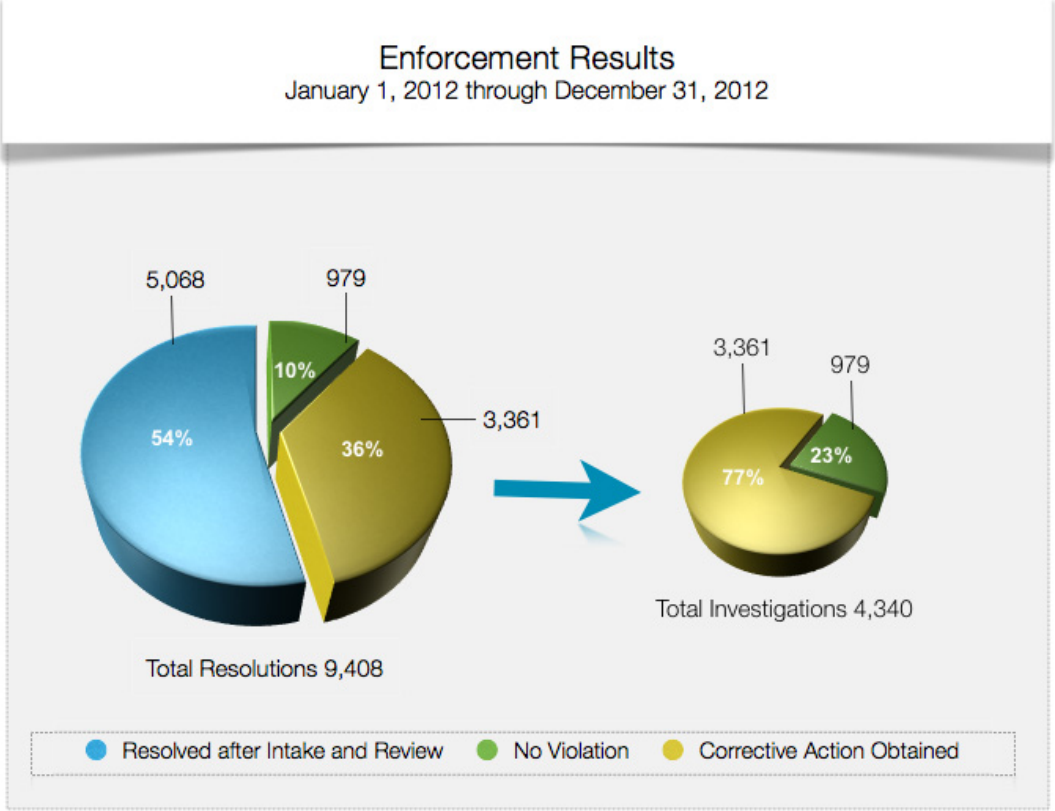
Although OCR resolved over ninety-one percent of the complaints received since the compliance dates of the HIPAA Rules by the end of calendar year 2011, a remainder of approximately 5,983 open complaints carried over into calendar year 2012. During calendar year 2012, OCR received an additional 10,454 complaints, a significant increase of 1,432 complaints over the previous year's all-time high. OCR resolved a total of 9,408 complaints.

In 3,361 of the complaints investigated in 2012, OCR either provided technical assistance to the covered entity, and/or required the covered entity to take corrective action. In 979 of the complaints investigated, OCR found that no violation of the HIPAA Rules had occurred. Finally, in 5,068 complaints, 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

[8] 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.

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.

During calendar year 2012, OCR opened at least 235 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints. Of these, 222 compliance reviews were opened as a result of a breach report affecting 500 or more individuals.[9]



[9] *Id.*

Significant Activities: Resolution Agreements, CMPs, and Subpoenas[10]

Resolution Agreements

Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc.

On February 14, 2011, the Department reached agreement with General Hospital Corp. and Massachusetts General Physicians Organization, Inc. (Mass General) to settle potential violations of the Privacy Rule. To resolve the Department's investigation of its privacy practices, Mass General agreed to pay $1,000,000 and to implement a detailed corrective action plan (CAP) to ensure that its workforce members appropriately protect and safeguard PHI.

The incident giving rise to the agreement involved the loss of protected health information (PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR's investigation indicated that Mass General failed to implement reasonable and appropriate safeguards to protect the privacy of PHI when the information was removed from Mass General's premises and lost.

The incident involved the loss of documents consisting of a patient schedule containing names and medical record numbers for a group of 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of those patients. These documents were lost on March 9, 2009, when a Mass General employee commuting to work left the documents on a subway train. The documents were never recovered.

Under the resolution agreement, Mass General agreed to pay a $1,000,000 resolution amount and implement a strong CAP that requires:

- developing and implementing a comprehensive set of written policies and procedures governing: (1) physical removal and transport of PHI; (2) laptop encryption; and (3) USB drive encryption to ensure PHI is protected when removed from the premises;

- distributing policies and procedures to all current and new workforce members;

- training workforce members on policies and procedures;

- engaging an internal monitor to assess Mass General's implementation and compliance with the CAP as well as render semi-annual reports to the Department; and

[10] 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.

- submitting compliance reports to the Department for a period of three years.

Resolution Agreement with the University of California at Los Angeles Health System

On July 6, 2011, the Department reached agreement with the University of California at Los Angeles Health System (UCLAHS) to settle potential violations of the Privacy and Security Rules. To resolve the Department's investigation, UCLAHS agreed to pay $865,500 and committed to a CAP aimed at remedying gaps in its compliance with the HIPAA Rules.

The resolution agreement resolves two separate complaints filed with the Department on behalf of two celebrity patients who received care at UCLAHS. The complaints alleged that UCLAHS employees repeatedly and without a permissible reason looked at the ePHI of these patients. In addition, the Department's investigation into the complaints revealed that from 2005-2008, unauthorized employees repeatedly looked at the ePHI of numerous other UCLAHS patients.

The resolution agreement requires UCLAHS to implement policies and procedures that reasonably restrict patient information access to only those employees with a valid reason to view the information and must sanction any employee who is found to have violated these policies and procedures.

Under the resolution agreement, UCLAHS agreed to pay an $865,500 resolution amount and implement a strong CAP that includes:

- developing and implementing written policies and procedures regarding restricting access to patient PHI and sanctioning workers who do not follow them;

- training workforce members on these new requirements; and

- engaging a qualified, independent third-party monitor to, among other duties, conduct compliance reviews, and render semi-annual reports to the Department for a period of three years.

Resolution Agreement with Blue Cross Blue Shield of Tennessee

On March 9, 2012, the Department reached agreement with Blue Cross Blue Shield of Tennessee (BCBST) to settle potential violations of the Privacy and Security Rules. To resolve the Department's investigation, BCBST agreed to pay $1,500,000 and agreed to implement a CAP to address gaps in its HIPAA compliance program. The enforcement action was the first resulting from a breach report required by the HIPAA Breach Notification Rule.

The investigation followed a notice submitted by BCBST to the Department reporting that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the PHI of over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR's investigation indicated BCBST failed to implement appropriate administrative safeguards to

adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls. Both of these safeguards are required by the HIPAA Security Rule.

Under the resolution agreement, BCBST agreed to pay a $1,500,000 resolution amount and implement a strong CAP that includes:

- reviewing, revising, and maintaining its HIPAA Privacy and Security policies and procedures;

- conducting regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA; and

- engaging a monitor to perform reviews to ensure BCBST compliance with the CAP.

Resolution Agreement with Phoenix Cardiac Surgery, P.C.

On April 13, 2012, the Department reached agreement with Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona (Phoenix Cardiac), to settle potential violations of the Privacy and Security Rules. To resolve the Department's investigation, Phoenix Cardiac agreed to pay $100,000 and to implement a detailed CAP to safeguard the PHI of its patients.

The incident giving rise to OCR's investigation was a report that the physician practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible. On further investigation, OCR found that Phoenix Cardiac had implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules, and had limited safeguards in place to protect patients' ePHI.

OCR's investigation also revealed the following issues:

- Phoenix Cardiac failed to implement adequate policies and procedures to appropriately safeguard patient information;

- Phoenix Cardiac failed to document that it trained any employees on its policies and procedures on the Privacy and Security Rules;

- Phoenix Cardiac failed to identify a security official and conduct a risk analysis; and

- Phoenix Cardiac failed to obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI.

Under the resolution agreement, Phoenix Cardiac agreed to pay a $100,000 resolution amount and implement a strong CAP that includes:

- developing, retaining and revising its HIPAA Privacy and Security policies and procedures as necessary;

- conducting and documenting a risk analysis that complies with the HIPAA Security Rule;

- developing a risk management plan, as required by the HIPAA Security Rule, to address the risks identified by the risk analysis;

- identifying a security official who is responsible for the development and implementation of the policies and procedures and the HIPAA Security Rule; and

- training workforce members on the requirements of the HIPAA Rules.

Resolution Agreement with the Alaska Department of Health and Social Services

On June 25, 2012, the Department reached agreement with the Alaska Department of Health and Social Services (DHSS) to settle potential violations of the HIPAA Security Rule. To resolve the Department's investigation, Alaska DHSS agreed to pay the $1,700,000 and to take corrective action to properly safeguard the ePHI of its Medicaid beneficiaries.

OCR began its investigation following a breach report submitted by Alaska DHSS. The report indicated that a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of an Alaska DHSS employee. Over the course of the investigation, OCR found evidence that Alaska DHSS did not have adequate policies and procedures in place to safeguard ePHI. Further, the evidence indicated that DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.

Under the resolution agreement, Alaska DHSS agreed to pay a $1,700,000 resolution amount and implement a strong CAP that includes:

- developing, retaining, and revising its HIPAA Privacy and Security policies and procedures as necessary;

- conducting and documenting a risk analysis that complies with the HIPAA Security Rule;

- developing a risk management plan, as required by the HIPAA Security Rule, to address the risks identified by the risk analysis;

- training workforce members on the requirements of the HIPAA Rules; and

- engaging a qualified, independent third-party monitor to, among other duties, conduct compliance reviews, and render reports to the Department for a period of three years.

Resolution Agreement with Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc.

On September 13, 2012, the Department reached agreement with the Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (collectively referred to as "MEEI") to settle potential violations of the HIPAA Security Rule. To resolve the Department's investigation, MEEI agreed to pay $1,500,000 and to take corrective action to properly safeguard the ePHI of its patients.

The investigation by OCR followed a breach report submitted by MEEI, reporting the theft of an unencrypted personal laptop containing the ePHI of MEEI patients and research subjects. The information contained on the laptop included patient prescriptions and clinical information.

OCR's investigation indicated that MEEI failed to take necessary steps to comply with certain requirements of the HIPAA Security Rule, such as:

- conducting a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices;
- implementing security measures sufficient to ensure the confidentiality of ePHI that MEEI created, maintained, and transmitted using portable devices;
- adopting and implementing policies and procedures to restrict access to ePHI to authorized users of portable devices; and
- adopting and implementing policies and procedures to address security incident identification, reporting, and response.

OCR's investigation indicated that these failures continued over an extended period of time, demonstrating a long-term, organizational disregard for the requirements of the HIPAA Security Rule.

Under the resolution agreement, MEEI agreed to pay a $1,500,000 resolution amount and implement a strong CAP that includes:

- developing, retaining, and revising its HIPAA Privacy and Security policies and procedures as necessary;
- conducting and documenting a risk analysis that complies with the HIPAA Security Rule;
- developing a risk management plan, as required by the HIPAA Security Rule, to address the risks identified by the risk analysis;
- identifying a security official who is responsible for the development and implementation of the policies and procedures and the HIPAA Security Rule;

- training workforce members on the requirements of the HIPAA Rules; and

- engaging a qualified, independent third-party monitor to, among other duties, conduct compliance reviews, and render reports to the Department for a period of three years.

Resolution Agreement with the Hospice of North Idaho

On December 31, 2012, the Department reached agreement with the Hospice of North Idaho (HONI) to settle potential violations of the HIPAA Security Rule. To resolve the Department's investigation, HONI agreed to pay $50,000 and to take corrective action to properly safeguard the ePHI of its patients.

OCR began its investigation after HONI reported to the Department that an unencrypted laptop computer containing the ePHI of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of its field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve its HIPAA Privacy and Security compliance program.

Under the resolution agreement, HONI agreed to pay a $50,000 resolution amount and implement a CAP that includes reporting certain incidents to the Department for a two-year period.

Civil Money Penalties

Civil Money Penalty to Cignet Health of Prince George's County, Maryland

On February 4, 2011, the Department issued a Notice of Final Determination and Civil Money Penalty to Cignet Health of Prince George's County, Maryland (Cignet) for violations of the HIPAA Privacy Rule. The Department imposed a Civil Money Penalty (CMP) of $4.3 million for the violations, representing the first CMP issued by the Department for violations of the HIPAA Rules. The CMP is based on the violation categories and increased penalty amounts authorized by Section 13410(d) of the HITECH Act.

In a Notice of Proposed Determination, issued October 20, 2010, the Department found that Cignet violated 41 patients' rights by denying them access to their medical records when requested between September 2008 and October 2009. These patients individually filed complaints with the Department, initiating investigations of each complaint. The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient's request. The CMP for these violations was $1.3 million.

During the complaint investigations, Cignet refused to respond to the Department's demands to produce the records. Additionally, Cignet failed to cooperate with the Department's complaint investigations and produce the records in response to the Department's subpoena. Consequently,

the Department filed a petition to enforce its subpoena in United States District Court and obtained a default judgment against Cignet on March 30, 2010.[11] On April 7, 2010, Cignet produced the medical records, but otherwise made no efforts to resolve the complaints through informal means.

In addition, the Department found that Cignet failed to cooperate with its investigations on a continuing daily basis from March 17, 2009, to April 7, 2010, and that the failure to cooperate was due to Cignet's willful neglect to comply with the HIPAA Rules. Covered entities are required under law to cooperate with the Department's investigations. The CMP for these violations was $3 million.

On August 4, 2011, represented by the U.S. Attorney for Maryland, the Department filed a complaint in U.S. District Court of Maryland to collect the CMP. Cignet opposed the collection action. On August 31, 2012, the district court issued an order entering a judgment for the Department in the amount of $4,782,845 for the CMP and the costs of litigation against Cignet and its owners as the partners of the forfeited corporation. Subsequently, on January 16, 2013, the 4th Circuit Court of Appeals dismissed Cignet's appeal. The Financial Litigation Unit (FLU) in the United States Attorney's Office in Maryland is actively working to collect on the judgment. The Department continues to monitor the FLU collection activity.

Subpoenas

On March 3, 2011, OCR issued an investigative subpoena to a company that operates a social networking website seeking any documents that may be in its possession pertaining to any accounts which may have been held by or in the name of a doctor during the period from June 1, 2006, through July 31, 2006. OCR was investigating a complaint alleging that the doctor impermissibly disclosed an individual's PHI by posting a photograph of the individual on the website, together with a statement about the individual's health condition. The subpoena was issued by OCR pursuant to its subpoena authority under HIPAA (42 U.S.C. 1320d-5, 1320a-7a(j)). The company operating the website responded to the subpoena stating that it was unable to comply with the request due to insufficient information. OCR supplied the additional information requested by the company, and on July 31, 2012, the company supplied the subpoenaed information. Thereafter, OCR determined that there was insufficient evidence to support the complaint allegations.

Audits

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 Privacy and Security 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

[11] *See* the Report to Congress on Compliance with the HIPAA Privacy and Security Rules for calendar years 2009 and 2010 (August 11, 2012): http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereptmain.html.

application of a set of objective selection criteria. Through the use of funds available under American Recovery and Reinvestment Act of 2009, OCR, with the help of different federal government contractors, undertook several projects to begin its audit program, including: initiating a study to determine the most effective means of implementing an audit program; developing a database of HIPAA covered entities to audit; drafting a protocol for a pilot audit program; conducting an audit pilot project; and completing an evaluation study of the pilot audit program (an activity that continued into 2013).

Overall, the audit program is a powerful augmentation of OCR's health information privacy and security compliance program. OCR will use the audit program to assess HIPAA compliance efforts at a broad range of covered entities and business associates. Audits present a new 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.

OCR engaged the services of a professional public accounting firm to conduct the performance audits, using generally accepted government auditing standards. The pilot audit program was a three-step process.

In the first step, audit protocols were developed to analyze the processes, controls, and policies of covered entities. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements varied based on the type of covered entity selected for review. The Privacy Rule protocol covers: (1) notice of privacy practices for PHI; (2) rights to request privacy protection for PHI; (3) access of individuals to PHI; (4) administrative requirements; (5) uses and disclosures of PHI; (6) amendment of PHI; and (7) accounting of disclosures. The protocol for Security Rule requirements covers administrative, physical, and technical safeguards. The protocol also covers requirements for the new Breach Notification Rule. The protocol is available for public review at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

Next, a limited number of audits were conducted to test and "fine tune" these protocols. These initial audits began in November 2011. The results of the initial audits helped to inform the remainder of the audits in the pilot audit program.

The last step included the conduct of audits of a range of entity types and sizes using revised protocol materials. The audits in the pilot program targeted a broad range of sizes and complexities of covered entities based on four levels, as outlined in the graphic below. (Business associates were not included in the pilot audits but will be addressed as part of future audits.)

Level 1 Entities consisted of:

- Large Provider / Health Plan
- Extensive use of HIT-complicated HIT enabled clinical business work streams
- Revenues and or assets greater than $1 billion

Level 2 entities consisted of:

- Large regional hospital system (3-10 hospitals/region) / Regional Insurance Company
- Paper and HIT enabled work flows
- Revenues and or assets $300 million to $1 billion

Level 3 Entities consisted of:

Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entitied that don't adjudicate their claims

- Some but not extensive use of HIT - mostly paper based workflows
- Revenues $50 million to $300 million

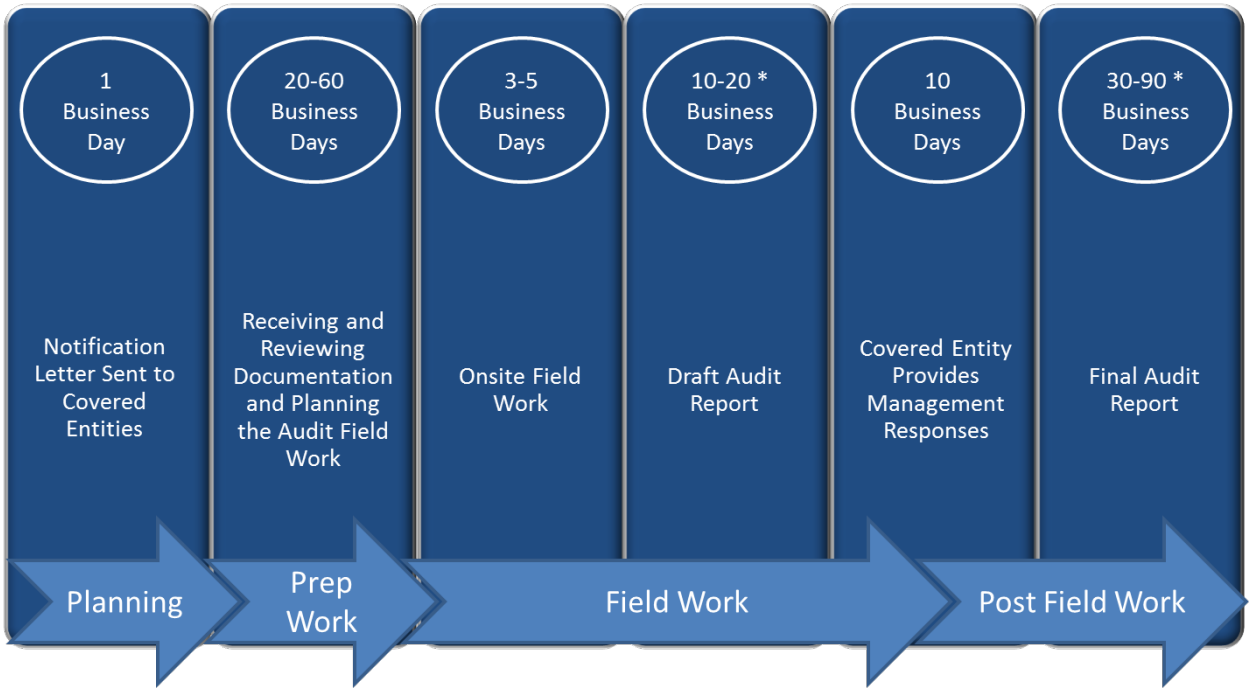
Level 4 Entities consisted of:

- Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)
- Little to no use of HIT - almost exclusively paper based workflows
- Revenues less than $50 million

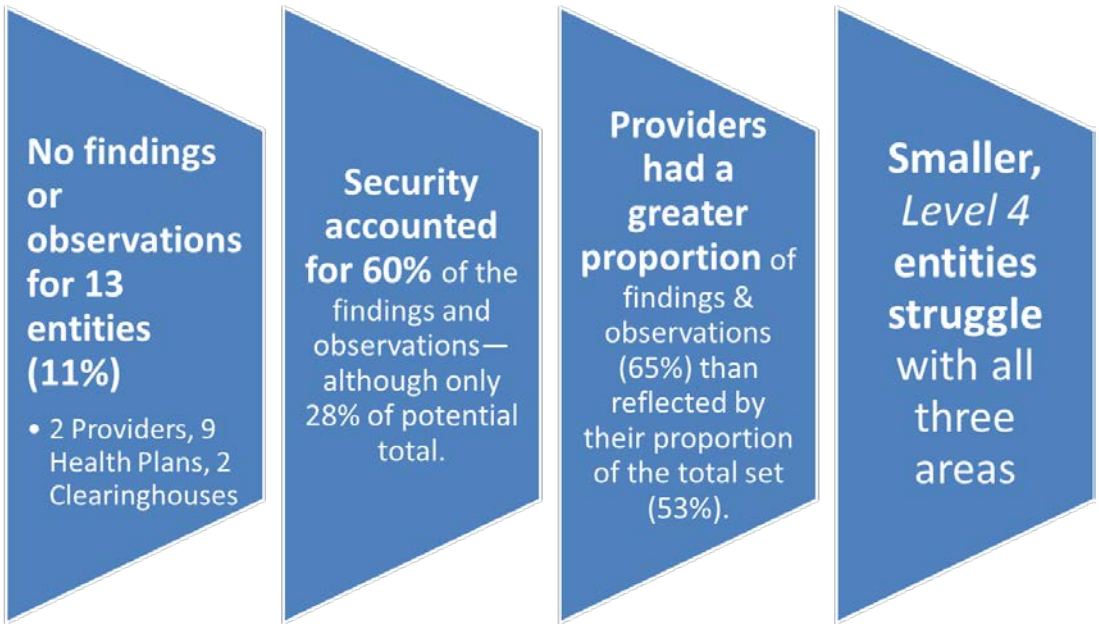
The 115 covered entities audited included: 47 health plans, 61 health care providers, and 7 health care clearinghouses.

	Level 1	Level 2	Level 3	Level 4	Total
Health Plans	13	12	11	11	47
Health Care Providers	11	16	10	24	61
Health Care Clearinghouse	2	3	1	1	7
Total	26	31	22	36	115

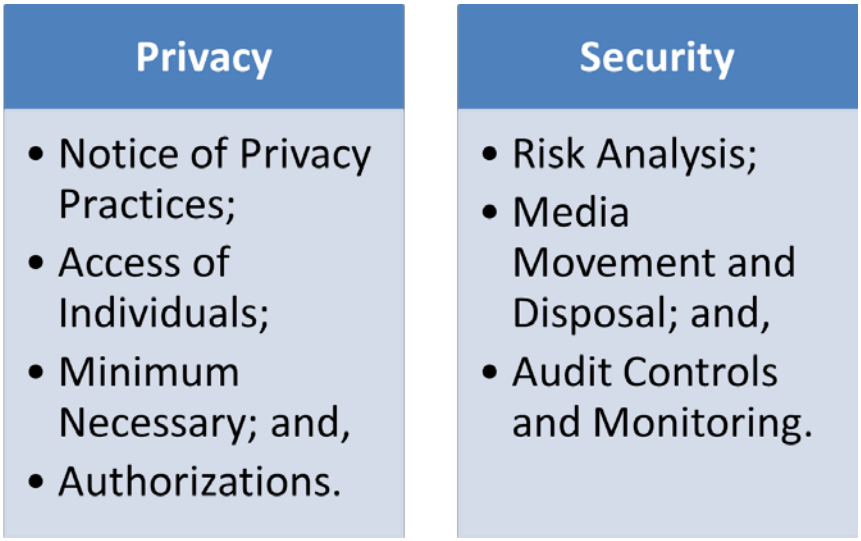
The pilot audits generally utilized the following process:



All audits in this pilot were completed by the end of December 2012. The results of the pilot, as illustrated below, are informing OCR's audit program going forward. While there were no findings or observations for 13 entities (11%), the majority of entities audited, particularly small entities, continued to show deficiencies with regard to all three of the HIPAA Rules—Privacy, Security, and Breach Notification.



As illustrated below, the specific requirements of the Privacy Rule where audited covered entities fell short included those provisions of the Privacy Rule addressing the rights of individuals to: receive a Notice of the privacy practices of the covered entity; access their protected health information; and authorize disclosures of their protected health information. Also, audited covered entities lack effective Security Rule compliance programs, specifically with regard to: assessing the risks to their ePHI, implementing protections for removable media that stores ePHI and controlling and monitoring access to ePHI. OCR has focused its outreach and technical assistance to address these areas of the HIPAA Rules, as is discussed further in the next section of the report.



Finally, a discussion of the audit findings with regard to covered entities' deficiencies in compliance with the requirements of the Breach Notification Rule are discussed in the a separate Report to Congress, available at http://www.hhs.gov/ocr/privacy/.

Plans for Future Improved Enforcement

Significant Enforcement Action

Moving forward, OCR intends to realign its enforcement efforts to focus its limited resources on cases that present OCR with the maximum opportunity to effect change within the health care industry. In the past, OCR has attempted to review and resolve the alleged violations in all complaints received, either by determining that OCR does not have jurisdiction, or by starting an investigation to: determine that a particular HIPAA covered entity or business associate did not violate the HIPAA Rules; provide technical assistance to a particular covered entity or business associate; or require that a covered entity or business associate make changes to its policies, procedures, and practices.

OCR will continue to review all complaints to determine whether the complaint alleges conduct over which OCR has jurisdiction, whether a particular complaint is appropriate for investigation

by one of OCR's ten regional offices, or whether the complaint can be resolved effectively by providing technical assistance to the covered entity or business associate without investigation.

Given OCR's experience with an ever-increasing volume of complaints, without a corresponding increase in resources, OCR is determining ways to "work smarter," that is, to increase the effectiveness of its allocation of staff time and other resources to achieve the most industry compliance with the HIPAA Rules. Many complaints can be resolved more effectively through early intervention and technical assistance than through an investigation. For example, in complaints where a particular individual experiences problems gaining access to his or her protected health information, OCR staff can intervene effectively on the individual's behalf by providing technical assistance to the HIPAA covered entity involved and facilitating timely access for the individual without opening an investigation. This allows OCR to focus its investigatory work on those cases that present compliance issues that are pervasive in the health care industry or other serious allegations and to engage the covered entities and business associates in these cases to reach meaningful resolution.

Finally, OCR significantly increased its efforts to move forward with investigations of complaints and compliance reviews that will result in a substantial industry impact ("high-impact cases") to encourage compliance with the HIPAA Rules during calendar years 2011 and 2012. During these two years, OCR entered into seven resolution agreements that include monetary settlement amounts, and extensive correction action plans to resolve high-impact cases involving the HIPAA Rules, and assessed civil money penalties in one case. While this represents a very small fraction of the complaints and compliance reviews through which OCR investigates compliance with the HIPAA Rules, this is double the number of high-impact cases that OCR resolved through resolution agreements and corrective action plans from 2008 to 2010. OCR continues to work aggressively to identify and investigate high-impact cases that send strong enforcement messages about important issues involved in complying with the HIPAA Rules. OCR will continue this uncompromising enforcement posture into the future.

In its enforcement efforts, OCR continues to work diligently with other federal agencies, including the Federal Trade Commission, DOJ, the Department's Office of the Inspector General (OIG), and the State Attorneys General, to enforce the HIPAA Rules. OCR continues to refer all complaints involving criminal allegations of the HIPAA Rules to the DOJ, has worked with the OIG on HIPAA implications of health care fraud investigations, and recently developed a model information-sharing agreement to promote information-sharing with the State Attorneys General in enforcement investigations.

Audits

Through 2013, OCR analyzed the findings of the audits for trends, potential best practices, and vulnerabilities. In addition, OCR engaged Price Waterhouse Cooper (PWC) to conduct an evaluation of the audit program. The evaluation included surveys of audited entities, review of the protocols, and examination of the program structure and documentation. OCR received the final report from PWC in November 2013. OCR is using the recommendations and findings from the evaluation report to finalize plans for the audit program moving forward.

OCR is committed to integrating the next round of audits into its program during 2014. OCR is updating the audit protocol to reflect the new requirements implemented through the January 25, 2013, final rule and will post it to the OCR website, so covered entities and business associates can use the updated protocol for their own internal compliance assessments. Other activities include development of additional guidance responsive to issues found through the audits. Audits in 2014 will focus on particular requirements of the HIPAA rules and specific subsets of covered entities and business associates.

This comprehensive approach to the creation of OCR's Audit Program is intended to help ensure the final audit protocols are effective, accurate, and objectively neutral for the measurement of compliance across covered entities and business associates.

Extensive 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 covered entity community identified by complaint investigations, compliance reviews, and the pilot audit program, OCR significantly amplified its public outreach and education campaign beginning in 2010 and continuing to today, with the goal of increasing compliance with the HIPAA Rules across the health care industry. OCR's efforts have included:

- An incredibly popular YouTube channel that features videos for HIPAA covered entities and their business associates, and for both English- and Spanish-speaking consumers.

- A Medscape "Resource Center," which contains modules that offer free Continuing Medical Education (CME) credits for physicians and Continuing Education (CE) credits for health care professionals.

- The "Information is Powerful Medicine" Campaign, which aims to increase awareness of HIPAA rights and benefits among patients living with HIV.

- A set of multi-language fact sheets developed to inform consumers about their rights under the HIPAA Privacy Rule.

- A "HIPAA Guide for Law Enforcement," which describes the HIPAA Privacy Rule, identifies entities that are not required to comply with the HIPAA Rules, and outlines several disclosure permissions that allow the disclosure of PHI to law enforcement in common law enforcement situations, such as during an emergency response.

- Multiple guidance documents and related resources for HIPAA covered entities and business associates, including: guidance addressing mobile device security, model notices of privacy practices, and a tool to help small providers comply with the HIPAA Security Rule's requirement to perform a risk analysis, developed in coordination with the Office of the National Coordinator for Health IT; sample business associate agreement provisions; guidance on de-identification under the HIPAA Privacy Rule; and fact sheets on marketing and refill reminders and other topics under the HIPAA Privacy Rule.