**Testimony**
**Before the Committee on the Judiciary**
**Subcommittee on Privacy, Technology and the Law**
**United States Senate**

*Statement of*

# Leon Rodriguez

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

**For Release on Delivery**
**Expected at 2:30 p.m.**
**Wednesday, November 9, 2011**

## Introduction

Mr. Chairman and members of the Subcommittee, it is an honor for me to be here today in my capacity as the Director of the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS). The privacy and security of personal health information is essential to and at the core of the work of HHS to improve access to and the quality of the health care provided to individuals. OCR administers and enforces the health information Privacy, Security, and Breach Notification Rules, issued under the Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, and the Health Information Technology for Economic and Clinical Health (HITECH) Act. In doing so, we play an important role in ensuring that individuals' sensitive health information remains private and secure, and that individuals have important rights with respect to their health information. I thank you for the opportunity to testify today on the role of the HIPAA Privacy, Security, and Breach Notification Rules in the protection of individuals' health information maintained in electronic health records and elsewhere.

HIPAA established a national, uniform baseline of privacy and security protections for individuals' health information, and the HITECH Act, part of the American Recovery and Reinvestment Act, strengthened and expanded these protections. The HITECH Act's unprecedented investment in health IT has greatly accelerated the adoption of electronic health records (EHRs) among providers and supported efforts to rapidly build capacity for exchanging health information. At the same time, the HITECH Act acknowledged that, to achieve the full potential of health IT to transform care, patients and providers must trust in the confidentiality of sensitive health information. To further that goal, the HITECH Act builds upon the framework of privacy and security protections established by HIPAA. I will provide a brief overview of the HIPAA Privacy and Security Rules, the HITECH Act modifications to HIPAA, and OCR's enforcement of these protections.

## Background

HIPAA was designed to improve the efficiency and effectiveness of the health care system by promoting the electronic exchange of health information. At the same time, Congress

recognized that advances in electronic technology, if not properly regulated, could erode the privacy and security of that health information. To address this, Congress incorporated provisions into HIPAA requiring the adoption of Federal privacy and security protections by certain health care providers, health plans, and health care clearinghouses. The HIPAA Privacy Rule requires these entities, known as covered entities, to have safeguards in place to ensure the privacy of individuals' identifiable health information. The rule also sets forth the circumstances under which covered entities may use or disclose an individual's information, and gives individuals rights with respect to their information, including rights to examine and obtain a copy of their health records and to request corrections. The HIPAA Security Rule requires covered entities to implement administrative, physical, and technical safeguards to protect health information in electronic form. The Rules also require HIPAA covered entities to contractually bind their business associates -- contractors or other persons hired to perform services for covered entities that involve individuals' health information -- to safeguard and only use or disclose the information as permitted by the Privacy Rule.

The HITECH Act not only promotes the adoption of health information technology and electronic health records but also works to build confidence in the privacy and security of the information in these records by strengthening and expanding HIPAA's privacy and security protections in a number of areas, such as by:

- Extending key responsibilities HIPAA placed on covered entities directly to their business associates, such as safeguarding and not misusing individuals' health information;
- Adding new requirements for notification of breaches of health information;
- Significantly strengthening HIPAA enforcement by increasing the civil money penalties for HIPAA violations and strengthening the Secretary's ability to act on HIPAA violations, particularly where there has been willful neglect;
- Strengthening individuals' rights to get an electronic copy of their health information;
- Generally prohibiting the sale of health information; and
- Further limiting the use and disclosure of personal health information for marketing and fundraising purposes.

The Department has issued a number of rules to implement these enhancements and is working hard to finalize those that remain in proposed form.

OCR enforces the HIPAA Privacy and Security Rules by investigating complaints from the public about potential violations of the Rules, as well as breach reports that covered entities are required by the HITECH Act to submit to the Secretary. OCR also may initiate an investigation in the form of a compliance review when privacy and security incidents are brought to our attention by the media, government agencies, or other sources. For the most part, the investigations are conducted by investigators in our 10 regional offices across the country. In addition to its investigations, OCR provides technical assistance to covered entities to foster compliance with the HIPAA Rules, and education and outreach to make the public aware of their rights under HIPAA. OCR is committed to expanding and improving its technical assistance and public education materials and finding new and innovative ways to communicate with all who have an interest in keeping health information private and secure.

OCR also coordinates HIPAA enforcement with the Department of Justice, which shares enforcement jurisdiction over HIPAA violations. HIPAA gives the Secretary of HHS the authority to impose civil money penalties for HIPAA violations, and the Department of Justice authority to enforce criminal violations. If a complaint implicates the criminal provision of HIPAA, OCR will refer the complaint to the Department of Justice. From April 2003, the date covered entities were required to be in compliance with the HIPAA Privacy Rule, to the end of September of this year, OCR referred 495 cases of potential criminal violations to the Department of Justice. Further, in cases in which the Secretary wishes to impose a civil money penalty, the Secretary is required to obtain prior authorization from the Attorney General of the United States.

OCR recently issued two annual reports to Congress, required by the HITECH Act, that describe in detail OCR's history of enforcement of the HIPAA Rules, as well as specific enforcement information for 2009 and 2010, and the number and nature of breaches that have been reported to the Secretary in 2009 and 2010 under the Breach Notification Rule. We also make available to

the public up-to-date enforcement data and information on our web site. I will now describe some of the highlights contained in the reports and on our web site.

**Enforcement of the HIPAA Privacy and Security Rules**

For most HIPAA covered entities, compliance with the Privacy Rule was required by April 14, 2003, and compliance with the Security Rule was required by April 20, 2005. The Secretary delegated the authority to administer and enforce the Privacy Rule to OCR, but initially delegated Security Rule enforcement to the Centers for Medicare & Medicaid Services. However, since that time, the Secretary recognized that the future increase in electronic health information as a result of the adoption of electronic health records would result in more cases that would implicate the HIPAA Security Rule, and would create an increased need for privacy and security to be addressed jointly. At the same time, having a unified enforcement approach to privacy and security would increase efficiency and result in better enforcement outcomes. Therefore, the Secretary re-delegated to OCR the authority to administer and enforce the HIPAA Security Rule on July 27, 2009.

From April 2003 through September of this year, HHS received more than 64,000 HIPAA Privacy Rule complaints and, since October 2009, we have received over 470 complaints alleging potential violations of the HIPAA Security Rule. The number of complaints that OCR receives has increased nearly every year since 2003, indicating a steadily increasing awareness and concern from the public about the privacy and security of their health information, and about their rights.

In about 15,000 of the more than 22,500 cases eligible for enforcement (*e.g.*, alleging a violation against an entity subject to the HIPAA Rules), we have required covered entities to make changes in privacy and security policies and practices, and to take other corrective actions. These actions have resulted in systemic changes that are designed to benefit all individuals served by the covered entities. The number of entities taking corrective action to resolve existing and prevent future compliance problems as a result of OCR enforcement continues to increase steadily each year. In the other 7500 cases eligible for enforcement, OCR investigations found no violation.

Since 2003, we have continued to see many of the same compliance issues through our investigations, and we have used our strongest enforcement tools to address some of these common issues.

For example, we see cases of employees inappropriately accessing patient information, in many cases in electronic data systems, for which they do not have a work-related need. These include hospital employees improperly accessing the health information of ex-spouses, friends, neighbors, or celebrities. Unlike paper systems, the audit trails of electronic systems enhance our ability to identify and track such privacy violations.

We also have seen multiple cases of improper disposal of records – whether it is pharmacies throwing prescription bottles and other health information away in dumpsters that are accessible to the public, or private practices going out of business and leaving patient records behind at their prior places of business.

Many cases involve providers failing to give individuals copies of their records, a fundamental right of individuals under HIPAA and a means of empowering consumers to engage in and manage their own health. Other cases involve misdirected communications, such as explanation of benefits mailings, often resulting from failures to test information systems or other system errors. I will discuss some of these cases in more detail later on in my testimony.

**Breach Reports to the Secretary**

The HITECH Act required the Secretary to issue breach notification requirements for HIPAA covered entities and their business associates. OCR issued a Breach Notification Rule as an interim final regulation in 2009, effective for breaches discovered on or after September 23, 2009. A breach is an impermissible use or disclosure of individuals' health information under the Privacy Rule which comprises the privacy or security of the information. The Rule requires covered entities to notify individuals, the Secretary, and in some cases, the media, of breaches of unsecured (*e.g.*, unencrypted) protected health information. In the case of a breach at a business associate of a covered entity, the Rule requires that the business associate inform the covered

entity of the breach so that the proper notifications can be made. As of November 4, 2011, OCR has received and posted on its website 364 reports of breaches involving more than 500 individuals.

Larger breaches commonly involve theft or loss of computers or electronic media housing unencrypted health information. For example, each of the six largest breaches this year involved the health information of between 175,000 individuals to over 4.9 million individuals. The three most extensive breaches, involving the health information of a total of almost 8 million individuals, were due to the loss of unencrypted backup media or disk drives. The next two largest breaches, which affected a total of over 900,000 individuals, resulted from the theft of desktop computers. Finally, one breach involving the health information of over 175,000 individuals resulted from a system error that misprinted several thousand documents.

Additionally, OCR has received over 36,000 reports of breaches involving fewer than 500 individuals. The majority of these reports involve misdirected communications and affected just one individual each. Often, the clinical or claims record or other health information of one individual is mistakenly mailed or faxed to another individual.

**Resolution Agreements and Civil Money Penalties**

The HITECH Act significantly strengthened the Department's ability to take enforcement actions against entities for HIPAA violations by revising and greatly increasing the civil money penalty amounts that may be imposed for violations. Prior to the HITECH Act, the Department had authority to impose on a covered entity a civil money penalty of up to only $100 for each violation, with a calendar year limit of $25,000 for all identical violations. The HITECH Act provided a stronger and more flexible the penalty scheme by creating four categories of violations that reflect increasing levels of culpability – from circumstances where the entity did not know of the violation to circumstances of willful neglect, and by attaching to each tier amounts that significantly increase the minimum penalty amount for each violation. Now, covered entities are subject to penalties that range from $100 to $50,000 or more per violation, with a calendar year limit of $1.5 million for identical violations. Our experience has been that the increased penalty amounts available to the Department have reinvigorated covered entities'

attention to compliance. The Department has authority to use these amounts not only for purposes of imposing civil money penalties but also for determining and negotiating settlement payments with covered entities that have agreed to resolve issues of noncompliance by entering into resolution agreements with the Department.

A resolution agreement is a contract between the Department and a covered entity to settle potential violations and is accompanied by a corrective action plan in which the covered entity agrees to perform certain obligations, such as retraining staff, and to make reports to the Department, generally for a period of three years. During the period, the Department monitors the covered entity's compliance with its obligations. These agreements are reserved to settle investigations with more serious issues and outcomes and generally include payment of a settlement amount. To date, HHS has entered into six resolution agreements. When a case cannot be resolved informally through corrective action, HHS seeks to impose a civil money penalty. Thus far, HHS has imposed a civil money penalty using the increased penalties amounts provided for by the HITECH Act on one covered entity. These cases are instructive for the health care industry because they involve some of the most common compliance issues that we see in our investigations.

For instance, OCR entered into resolution agreements -- in July 2008 with Providence Health and Services (Providence) and in February 2011 with General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (Mass Gen) -- after individuals' health information was stolen from or lost by employees taking the information offsite from the covered entity's premises. Providence and Mass Gen are important examples of the continuing problems that entities have with ensuring that proper safeguards and controls are in place with respect to employees removing and transporting patient information from the covered entity's facility. Providence paid a settlement amount of $100,000 and instituted a plan to revise policies and procedures, train employees, and to encrypt electronic health information on laptop computers and electronic media that are to be taken off the premises by employees. Mass Gen paid $1 million and instituted a plan to revise policies and procedures for employees taking patient information off-site, and training employees on these policies.

OCR also consistently encounters cases that illustrate the ongoing problem with proper disposal of patient information, whether it is in electronic or paper form. OCR entered into resolution agreements -- in January 2009 with CVS Pharmacy, Inc. (CVS), and in July 2010 with Rite Aid Corporation (Rite Aid) -- and obtained payments of $2.25 million and $1 million, respectively, to settle allegations of improper disposal of prescription bottles and other patient information. The investigations were carried out jointly with the Federal Trade Commission, which was investigating potential violations of the Federal Trade Commission Act. In the coordinated action, CVS and Rite Aid also signed consent orders with the FTC to settle the cases. In these cases, CVS and Rite Aid improperly disposed of patient information in unlocked dumpsters behind their retail stores, which were accessible to the public. We continue to work with covered entities to educate them about their responsibilities under the HIPAA Rules to safeguard patient information, including through disposal, and on the importance of ensuring employees know of the proper way to dispose of patient information.

Further, access to patient health information for marketing purposes continues to be a major concern of consumers, and is an issue that the HITECH Act specifically addresses. In December 2010, OCR entered into a resolution agreement with Management Services Organization Washington, Inc. (MSO) to resolve allegations of improper disclosure of patient information for marketing purposes. MSO was required to pay a settlement amount of $35,000. This case was coordinated with the Office of the Inspector General at HHS and with DOJ, which had been investigating MSO for violations of the Federal False Claims Act.

I spoke earlier about the frequency with which OCR encounters problems with hospital employees who inappropriately access information in the hospital's electronic data systems. In July of this year, the University of California at Los Angeles Health System (UCLA) entered into a resolution agreement with OCR and agreed to pay $865,500 to resolve allegations of UCLA employees repeatedly, and without permissible reasons, looking at the electronic health records of two different celebrity patients, as well as numerous other UCLA patients. The corrective action plan required UCLA to, among other things, conduct regular and robust trainings for all employees and implement policies to sanction offending employees.

Finally, one of our most important cases involved the fundamental HIPAA right of an individual to obtain a copy of his or her health information, and the blatant disregard of that right by a covered entity. In February of this year, with DOJ's approval and using the HITECH Act's strengthened penalty scheme, OCR issued a $4.3 million civil money penalty against Cignet Health of Prince George's County, MD (Cignet). Cignet refused to provide 41 patients with copies of their medical records when the patients requested them. Further, Cignet repeatedly failed to cooperate with OCR to resolve the issue, evidencing willful neglect with respect to compliance. OCR places a high priority on the ability of individuals to exercise their rights under HIPAA, and will not tolerate entities that refuse to provide individuals with their rights or cooperate with our investigations.

**Other Enforcement Activities**

*State Attorneys General*

OCR continues to leverage important relationships with the Department of Justice and with the Federal Trade Commission in its HIPAA enforcement work. In addition, OCR has been working with the State Attorneys General to coordinate enforcement. The HITECH Act gives State Attorneys General authority to enforce the HIPAA protections by bringing civil actions on behalf of State residents for violations of the HIPAA Rules. The State Attorneys General are authorized to seek injunctive relief or damages in the amount of up to $100 per violation, with a calendar year limit of $25,000 for identical violations. To assist them in their enforcement and to promote a productive and effective enforcement relationship with them, OCR conducted a series of HIPAA training seminars in four cities across the country, with representatives from over 45 States and territories, and the District of Columbia, in attendance. We continue to coordinate with the State Attorneys General, and in the past few months, have provided technical assistance on enforcement to the State Attorneys General in California, Connecticut, Illinois, Massachusetts, Michigan, Rhode Island, South Carolina, Texas, Washington, and Wyoming.

*Audits*

The HITECH Act authorizes HHS to conduct periodic audits to ensure that covered entities and business associates are complying with the HIPAA Privacy and Security Rules. As a result,

OCR, through the use of contract services, has begun to develop a pilot audit program and will be assessing its effectiveness. Audits will give OCR an ability to assess privacy and security protections and compliance issues on a systemic level, and to identify potential vulnerabilities to help entities prevent problems before they occur. This will complement the incident-based work that we currently conduct with respect to our investigations.

**Other Initiatives to Safeguard Health Information**

Many other efforts, in addition to OCR's enhanced enforcement activities, are underway to secure and protect highly sensitive patient health information as we move closer to the goal of the wide-spread adoption of electronic health record systems. One such initiative is the National Strategy for Trusted Identities in Cyberspace, signed by the President in April 2011, which calls for the development of a network of secure, interoperable digital credentials. Such digital credentials will enable patients and health care providers to access their electronic health records in a secure manner, and limit instances of inappropriate access as well as medical identity theft. Improving authentication is a key element to achieving the security requirements under the HIPAA Rules and realizing the full potential of the benefits that electronic health records can bring to society.

**Closing**

As you can see from my testimony, OCR is committed to ensuring the American public enjoys the full protections and rights afforded to them by the HIPAA Rules and to fostering a culture of compliance among the covered entities and business associates to whom individuals have entrusted their personal health information. These efforts also add to the public confidence that the investments being made in electronic health records, and the use of information to improve health, will be done in a way that also safeguards their privacy.

Mr. Chairman, this completes my prepared remarks and I will gladly answer any questions you or other members of the Committee may have at this time.