Testimony
Before the Energy & Commerce Committee
Subcommittee on Oversight and Investigations
United States House of Representatives

Statement of

Leon Rodriguez

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

For Release on Delivery
Expected at 10:00 a.m.
Friday, April 26, 2013

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). As HHS's enforcement agency for civil rights and health privacy rights, OCR investigates complaints, conducts compliance reviews, develops policy, promulgates regulations, and provides technical assistance and public education to ensure understanding of and compliance with non-discrimination and health information privacy laws.

OCR implements the health information privacy, security, and breach notification rules, under the Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, and the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH). In doing so, our office plays an important role in ensuring that individuals' sensitive health information remains private and secure, and that individuals are able to exercise important rights with respect to their health information. We also ensure that health information can flow for important and necessary purposes, such as patient treatment, obtaining payment for health care services, and protecting the public's health and safety.

I thank you for the opportunity to testify today about how the HIPAA privacy requirements apply to health care professionals and their interactions with patients and patients' family members and friends. I will provide a brief overview of HIPAA, describe how it applies to communications between health care providers and a patient's family and loved ones, and report on OCR's efforts to ensure that health care providers are fully aware of their ability under HIPAA to share information with those closest to the patient.

Background

HIPAA was designed to improve the efficiency and effectiveness of the health care system by promoting the electronic exchange of health information for administrative and financial health care transactions, such as submitting claims for treatment provided, or determining insurance eligibility. At the same time, Congress recognized that, without proper oversight, advances in electronic technology could erode the privacy and security of that health information. To address this, HIPAA requires certain health care providers, health plans, and health care

clearinghouses to adopt Federal privacy and security protections. The HIPAA Privacy Rule requires that these persons and organizations, known as covered entities, 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 health 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.

HITECH, in addition to accelerating the adoption of health information technology, also strengthened and expanded HIPAA's privacy and security requirements. For example, HITECH significantly bolstered HIPAA enforcement by extending liability for compliance with certain aspects of HIPAA to business associates of covered entities. HITECH also called for higher civil monetary penalties for HIPAA violations, and it augmented the Secretary's ability to act on HIPAA violations, particularly where there has been willful neglect. On January 25, 2013, HHS issued a Final Rule implementing these HITECH enhancements to the HIPAA Rules.

OCR investigates complaints from the public about potential violations of the Rules, as well as breach reports that HITECH requires covered entities to submit to the Secretary. OCR also may investigate privacy and security incidents that are reported by the media, government agencies, or other sources. OCR also provides technical assistance to covered entities to foster compliance with the HIPAA Rules, and education and outreach to make the public aware of its 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 a role in keeping health information private and secure.

Public Priorities

The HIPAA Privacy Rule carefully balances individual privacy interests with important public priorities with standards for when an individual's authorization is required to use or disclose personal health information. To achieve this balance, HIPAA includes a series of regulatory permissions allowing covered entities and business associates to use or disclose personal health information for specified purposes, without the individual's authorization. For example, HIPAA permits personal health information to be used or disclosed, without an individual's

authorization, for health care treatment and payment, and for the business operations of covered entities. HIPAA also permits uses and disclosures of individuals' health information that are required by other law, as well as for certain public health activities, for law enforcement purposes, and to avert serious and imminent threats to health or safety. Aside from these permitted disclosures, HIPAA requires disclosures in only limited circumstances – to HHS to ensure compliance with the Rule and to individuals to ensure they are able to access their own information.

I will discuss the ways in which HIPAA allows providers to share relevant information about a patient's health care with the patient's family members, friends, or others the patient wants involved in his or her care. I will also point out the instances in which a mental health or other health care provider may alert appropriate persons when a patient presents a serious and imminent threat to himself or others. Finally, I will outline OCR's efforts to ensure providers understand these important provisions.

Disclosures to Family Members and Friends

Recognizing the integral role that family and friends play in an individual's health care, the HIPAA Privacy Rule allows routine – and often critical – communications between health care providers and these persons. Unless the patient objects, health care providers may communicate with an individual's family members, friends, or other persons the individual has involved in his or her health care. If the patient is not present or is incapacitated, health care providers still may communicate with family and friends of the patient, if the provider determines, based on professional judgment, that doing so is in the best interest of the individual. I will share a few real-world examples to illustrate:

- A nurse can discuss a patient's medical condition in front of the patient's sister who accompanies the patient to an appointment;
- A pharmacist can give an individual's prescription to a friend whom the individual sends to pick up the prescription; and
- If a patient is unconscious or otherwise is incapacitated, the doctor can share information with family members or friends if the doctor determines, based on professional judgment, that doing so would be in the patient's best interest.

HIPAA also recognizes various individuals who serve as the patient's personal representative and have the right to access the patient's health care information, subject to certain limitations. Personal representatives generally include a parent or legal guardian of a minor child, or a legal guardian of an adult, who has authority to make health care decisions for the individual.

With respect to conversations between health care providers and patients' family members and friends, the HIPAA Privacy Rule respects an individual's wishes, to the extent practical and appropriate. This means that a health care provider is not permitted to share personal health information with the family members or friends of an adult individual who tells the provider not to do so. Protecting this core individual right under HIPAA is central to achieving HHS's goal of improving the Nation's health by fostering the public's trust in the health care system's ability and commitment to safeguard personal health information. The ability to assure individuals that their personal health information will remain private is particularly critical in the area of mental health care, where concerns about the negative attitudes associated with mental illnesses may affect individuals' willingness to seek needed treatment.

OCR has developed a number of resources over the years to educate health care providers and members of the public about these provisions, including dedicated pages on our website, as well as downloadable guides for both providers and patients, on this issue.
These resources are available on our website at
http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html.

"Duty to Warn"

As the President and my colleagues at HHS have emphasized in other venues, we know that most people who are violent do not have a mental disorder, and most people with a mental disorder are not violent. HHS's goals are to improve the identification of mental health disorders and the delivery of needed mental health services. With these goals in mind, HIPAA was designed to provide privacy and security protections to enable those who seek health care to do so in confidence, consistent with professional ethical standards in the medical community.

In those uncommon instances in which an individual poses a serious and imminent threat to himself or herself, or to another person, the HIPAA Privacy Rule allows a health care provider to alert appropriate persons of this threat, consistent with applicable law and their ethical "duty to warn." In particular, HIPAA permits a covered health care provider to share relevant information about a patient to a person or persons who are reasonably able to prevent or lessen the serious and imminent threat, consistent with applicable law and standards of ethical conduct. Depending on the circumstances, the alert could be directed to a law enforcement official, a family member of the individual, the target of the threat, and/or other persons.

This past January, as part of HHS's response to the tragic shooting in Newtown, Connecticut, and other recent events, OCR published a letter to the Nation's health care providers (http://www.hhs.gov/ocr/office/lettertonationhcp.pdf) to ensure that they are aware of their ability under HIPAA to disclose information, consistent with applicable law and their ethical "duty to warn," when they believe that a patient poses a serious and imminent threat to himself or others.

NICS ANPRM

On January 16, 2013, the President issued a series of Executive Actions to reduce gun violence across the Nation. Those actions included a commitment to address any unnecessary legal barriers, particularly relating to HIPAA, that may prevent states from reporting certain information to the national background check system for firearm purchases. The Brady Handgun Violence Prevention Act of 1993, and its implementing regulations, which established the background check system, prohibit several categories of individuals from possessing or purchasing firearms. One such category, the "mental health prohibitor," includes individuals who have been: (1) involuntarily committed to a mental institution; (2) found incompetent to stand trial or not guilty by reason of insanity; or (3) otherwise formally adjudicated as having a serious mental condition that results in the individual's presenting a danger to themselves or others or being unable to manage their own affairs. In response to the President's Executive Actions, OCR published (http://www.hhs.gov/news/press/2013pres/04/20130419a.html) an advance notice of proposed rulemaking (ANPRM) on April 23, 2013, to gather information about potential barriers HIPAA may pose to states reporting the identities of those individuals to the

background check system, and to solicit the public's feedback on the best way to address any barriers. In particular, we are considering creating an express permission in the HIPAA rules to permit certain covered entities to report the relevant information to the NICS. We encourage interested parties to submit comments during the comment period, which continues until June 7, 2013.

HIPAA Enforcement

Historically, providers often have been reluctant to share information with patients' friends and family members. Although HIPAA provides the avenues I described for disclosures to family members and friends, there may be other professional ethical obligations, State confidentiality laws, or internal policies of a health care organization, that affect whether health care providers are willing or able to share patients' personal health information with their families, friends, or others. In addition, while there are penalties under HIPAA for impermissibly disclosing individuals' health information or for failing to disclose when required, providers are not subject to penalties for declining to make disclosures that HIPAA merely permits. Still, the disclosure permissions are in the Rule for a reason, and, through guidance, we continue to encourage providers to use them.

With respect to OCR's enforcement of the HIPAA Rules, HITECH significantly strengthened HHS's ability to take enforcement actions against entities for HIPAA violations by revising and increasing the civil monetary penalty amounts that may be imposed for violations, reserving the highest penalties for those entities that demonstrate willful neglect of their obligations under the HIPAA Rules. Prior to HITECH, HHS could impose on a covered entity a civil monetary penalty of up to only $100 for each violation, with a calendar year limit of $25,000 for all identical violations. HITECH provided a stronger and more flexible penalty scheme by creating four categories of violations that reflect increasing levels of culpability and thus, higher minimum penalties – from circumstances where the entity did not know of the violation to instances involving willful neglect. Now, the penalties range from $100 to $50,000 or more per violation, with a calendar year limit of $1.5 million for identical violations.

Under this new structure, OCR largely concentrates its enforcement efforts on large, systemic failures to comply with the HIPAA Rules. In particular, as adoption of electronic health records becomes more widespread, we are working to ensure that health care entities implement reasonable and appropriate measures to safeguard individuals' health information in electronic form, as required by the HIPAA Security Rule. HITECH provided us with important tools in this effort, including the new civil monetary penalty structure I just described, which strengthens incentives for health care entities and their business associates to secure the information they maintain; and the breach notification requirements, which ensure that individuals and HHS learn about breaches of unsecured protected health information. We have found that many of the major breaches reported to us result from systemic shortcomings in entities' Security Rule compliance programs, and we are focusing our enforcement energy in this direction.

In contrast, be assured that OCR's enforcement efforts are not directed toward imposing penalties on health care providers who make good faith efforts to comply with the Privacy Rule with regard to communications with patients' family members and friends.

Closing

As you can see from my testimony, OCR is committed to ensuring both that the American public enjoys the full protections and rights afforded to them by the HIPAA Rules, and that information can be shared with the appropriate persons or authorities when it is consistent with individuals' wishes or necessary to protect their safety or the safety of the broader public.