Department of Justice

STATEMENT OF

LORETTA E. LYNCH
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

REGARDING

EXAMINATION OF THE ENFORCEMENT OF FEDERAL HEALTH INFORMATION PRIVACY LAWS

PRESENTED

NOVEMBER 9, 2011

Statement of
Loretta E. Lynch
United States Attorney
Eastern District of New York

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

Regarding Enforcement of Federal Health Privacy Information Laws
November 9, 2011

Chairman Franken, Ranking Member Coburn, members of the Subcommittee - Thank you for the opportunity to join our partners at the Department of Health and Human Services in discussing the Administration's efforts to enforce Federal laws protecting patient medical records. We consider patient privacy to be of utmost importance for many reasons. Strong privacy protections help ensure that patients are candid with their doctors and other health care providers so that they receive the care they need. Privacy breaches chip away at the confidential patient-physician relationship, erode patient candor, and thus interfere with medical professionals as they gather the information they need to deliver accurate, quality, and thorough medical care.

Unauthorized access to medical records can have many other profound repercussions for patients, as well as for public and private health plans, medical providers, financial institutions, and other businesses. For patients, the public disclosure of intimate details of personal medical conditions or treatments can be devastating, with consequences ranging from profound embarrassment and humiliation to the loss of employment. Moreover, when stolen patient identities are used in a scheme to bill for

medical services that are never provided, future health care and health benefits may be affected. False treatment information memorialized in a patient's records can fatally distort the diagnosis of a future medical affliction. Future critical medical services may be denied by a health plan on the basis of an earlier-billed phantom surgery or durable medical equipment.

In addition, a patient can be negatively affected by the destruction of a hard-earned credit rating, destroyed as a consequence of fraudulently opened credit card accounts or bogus loans. And finally, record breaches can result in significant financial losses to government and private health care plans, financial institutions, and other businesses, oftentimes in the millions of dollars. Protecting patients' health records is especially critical as our country rapidly moves to improve our capacity to provide quality health care for all and to reduce costs, in part through the use of electronic medical records.

Coordination between the Departments of Justice and Health and Human Services

To successfully deter and punish breaches of medical record privacy, interagency cooperation between the Departments of Justice and Health and Human Services is critical. Congress has provided a wide range of administrative, civil and criminal tools with which medical records breaches can be addressed. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as recently strengthened by the commonly named "HITECH amendments" included in the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5), provides three distinct tools to enforce HIPAA's protections:

- First, the Secretary of the Health and Human Services, with DOJ concurrence, is empowered to impose civil monetary penalties ("CMPs"), which can amount to $50,000 or more per violation and up to a total of $1,500,000 in a single calendar year, for repeated violations of a provision of the medical privacy and security rules;
- Second, under a new authority added by the 2009 HITECH amendments, State attorneys general can initiate civil proceedings for injunctive relief. Damages on behalf of a State's citizens for violation of HIPAA medical privacy provisions can be up to $25,000 in a calendar year; and
- Third, the Department of Justice can investigate and prosecute HIPAA violations under the HIPAA criminal statute found at 42 U.S.C. § 1320d-6. The most egregious violations of HIPAA are subject to a period of incarceration up to 10 years, and a statutory fine up to $250,000.

Because HIPAA provides these multiple enforcement options to penalize privacy breaches, coordination among the enforcers is necessary. Pursuant to an informal agreement between the Departments of Justice and Health and Human Services, the Federal Bureau of Investigation ("FBI") routinely coordinates with the Office for Civil Rights of the Department of Health and Human Services ("HHS-OCR") regarding complaints filed with HHS-OCR that may represent a HIPAA criminal violation. While the FBI has jurisdiction for the investigation of criminal violations of the medical privacy law, HHS-OCR has responsibility for medical privacy and security violations that are civil in nature. HHS-OCR has an established process for receiving complaints of potential HIPAA violations from the public and also receives information about potential

violations through self-disclosure from health care providers and other covered entities. By agreement with the Department of Justice, HHS-OCR forwards to the FBI all HIPAA complaints or disclosures involving potential criminal violations. HHS-OCR then refrains from taking any action until the FBI reviews the referral, conducts any necessary investigation, and obtains an assessment from the local United States Attorney's Office. If the U.S. Attorney's Office declines a matter, it is returned to HHS-OCR for investigation and potential assessment of a CMP. Similarly, if the FBI or U.S. Attorney's Office concludes that a matter reported directly to the Department of Justice does not warrant criminal prosecution, it can be referred over to HHS-OCR for potential action.[1]

Before the Recovery Act enhanced HIPAA's enforcement tools, the Secretary was obligated to refer virtually every HIPAA complaint it received involving a potential criminal violation of HIPAA to the Department of Justice for evaluation for criminal prosecution. This dynamic was the consequence of a pre-Recovery Act provision of the HIPAA statute which prohibited the Secretary from imposing a civil money penalty (CMP) if "the act constitutes an offense punishable under [the HIPAA criminal statute]." Given the nearly identical offense language predicate for assessing a CMP and for charging a HIPAA misdemeanor offense, a large universe of potential HIPAA offenses, which had not been committed under fraudulent pretenses, to inflict harm or for personal or commercial gain, were referred even though they were susceptible to more efficient

[1] On occasion, we receive direct referrals from sources other than HHS-OCR. For example, we have received referrals from local law enforcement agencies who find abandoned medical records in office building dumpsters. Medical providers and health insurance plans that discover that their computers have been hacked and records stolen have also reached out to Federal law enforcement. We have also received referrals directly from health care providers who were subject to a corporate integrity agreement entered with the HHS Office of Inspector General as a consequence of an unrelated health care fraud.

resolution under the civil monetary penalty statute. In an abundance of caution, a much larger number of referrals were sent to the Department of Justice than would have otherwise been made. This decline in criminal referrals has continued in recent years – there were 13 referrals in fiscal year 2010 and 16 referrals in fiscal year 2011.

Common Schemes to Steal Medical Records

The subset of medical record privacy breaches that warrant criminal enforcement generally tend to fall into one of three fact patterns. First, we have prosecuted criminally when medical records and identities were stolen to commit massive health care frauds. We have found that these cases cause grave societal harm, both because the patients' historic medical and insurance records are corrupted and because there are often massive losses, profoundly draining precious health care payment resources. Recently, indictments were unsealed in the Southern District of New York and four other Districts charging seventy-three defendants, including a number of alleged members and associates of an Armenian-American organized crime enterprise, with various health care fraud-related crimes involving more than $163 million in fraudulent billing. The health care fraud scheme was allegedly accomplished through the theft of the identities of doctors and thousands of Medicare beneficiaries through the operation of at least 118 different phony clinics in 25 States for the purposes of submitting Medicare reimbursements. Racketeering charges were included, predicated in part on identity theft and access device fraud.

Second, we have prosecuted when medical records were stolen for the purpose of embarrassing or threatening to embarrass a particular patient or health care entity – for example, to attack the credibility of the patient publicly, to sell the records of a celebrity

patient to a media outlet, or to extort ransom payments to avert the disclosure of customers' health records. For example, this past June in the District of Arizona, a defendant was sentenced after pleading guilty to violating the HIPAA privacy statute by accessing sensitive medical and psychiatric records of several State employees who were involved in a State administrative hearing to which she was a party. The defendant then disclosed this information by including it in a letter that she sent to the Governor to complain about a State agency's use of employees with psychiatric records.

Similarly, in December 2008, an administrative assistant at the UCLA Medical Center in Los Angeles pleaded guilty in the Central District of California to illegally obtaining protected health records after she received at least $4,600 from a media outlet in exchange for providing the private medical information of a celebrity patient at the facility. And in September 2009, an Indianapolis defendant was sentenced to three years in prison for stealing insurance records of over 900,000 individuals. The records included personally identifiable information, confidential medical information, and confidential email communications. The defendant had threatened to publish this personal information and confidential medical data on the Internet, unless each victim insurance company paid him $1,000 per week for four years.

Finally, we bring criminal medical record theft cases where the ultimate motive was financial fraud against financial institutions or other businesses. Two recent cases from the District of Maryland illustrate this type of theft and fraud. In 2010, five defendants were indicted in Maryland for a fraudulent credit card scheme using information stolen from Johns Hopkins Hospital patient records. The indictment charged that more than 50 businesses and individuals were victimized. Earlier this year, a Federal

grand jury in Baltimore indicted four defendants, including a former employee of the University of Maryland Medical Center, in connection with a scheme in which the identifying information of medical center patients and others was stolen and used to defraud financial institutions. As another example, in the Southern District of Florida in 2009, we convicted two defendants of offenses related to the theft of patient records from Palmetto General Hospital designed to further a credit card fraud scheme.

We see other criminal activity involving the theft of medical records as well, although less frequently. For example, the theft of a laptop or other computer equipment, where the motive may have been to just steal computer equipment, can include the unknowing theft of electronic medical information data on tens of thousands of patients. We have also prosecuted medical identity theft where the primary purpose of the scheme was to prepare and submit multiple fraudulent tax returns.

Various Statutes Used to Prosecute

Because the fact patterns involved in medical records privacy cases are so varied, the criminal statutes used to prosecute medical records privacy cases are also varied. In fact, cases charging just a violation of the HIPAA criminal statute, 42 U.S.C. § 1320d-6, are a small portion of our cases involving breaches of medical privacy. We often bring such cases under identity theft and unlawful computer access statutes rather than the HIPAA statute. When appropriate, we also bring an aggravated identity theft charge that carries a mandatory two year sentencing enhancement. Some prosecutions focus on the payment for the disclosed medical records and charges are brought under the Medicare anti-kickback statute. We also may charge defendants under the general conspiracy statute through which we may be able to reach a wider range of defendants. And we have

charged violations of the general health care fraud statute as well in medical records privacy cases. Differing fact patterns among cases will guide a prosecutor's choice of charging statutes.[2]

This wide range of fact patterns and statutes used to charge those who breach the privacy of medical patients makes the task of accurately capturing all of the cases prosecuted by the Department in this area a difficult one. The Department's case tracking systems are organized by principal charging statute; as such, they do not allow us to track precisely all medical privacy breach cases prosecuted where a statute other than the HIPAA statute was the primary one contemplated or charged. Nevertheless, we can report that the FBI currently has 56 pending investigations associated specifically with violations of the HIPAA statute. In addition, during fiscal year 2011, Federal prosecutors working with the FBI brought cases charging 16 individuals and obtained 16 convictions in cases under HIPAA as reflected in the FBI's case tracking system. The FBI also obtained one additional medical privacy breach conviction in a case it worked with local prosecutors. Again, these numbers do not include any additional cases in which a medical record privacy breach occurred but the HIPAA statute was not the primary one charged. In addition, as noted above, these numbers reflect only those cases where criminal prosecution, as opposed to a civil or administrative remedy, was deemed the most appropriate enforcement option.

[2] One additional factor may have previously influenced some prosecutors to bring medical privacy cases under non-HIPAA statutes. In 2005, the Department's Office of Legal Counsel ("OLC") issued an opinion concluding that in most situations only "covered entities" (medical providers, health plans and health care clearing houses) could be prosecuted directly under HIPAA. Others, such as the employees of covered entities, could not be prosecuted directly under the statute according to OLC. The HITECH amendments in 2009 subsequently removed this impediment to prosecution by amending the HIPAA statute to reach employees of covered entities, as well as other individuals.

Conclusion

Our track record in prosecuting health care privacy cases demonstrates the seriousness with which we take the unlawful breach of medical privacy and our commitment to investigate and prosecute these cases criminally when the facts warrant criminal sanction. The Department of Justice looks forward to continuing to work in this important area with Congress and with our partners at the Department of Health and Human Services.

Thank you for affording me the opportunity to testify today. I would be pleased to answer any questions you might have.