

## QUESTIONS FOR THE RECORD

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

“Does HIPAA Help or Hinder Patient Care and Public Safety?”

April 26, 2013

Committee on Energy and Commerce, Subcommittee on Oversight and Investigation, U.S. House of Representatives

The Honorable Tim Murphy

### Question 1:

**In your prepared testimony, you wrote: “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.” What will your office do, after this hearing, to make sure this is more widely known?**

OCR's focus is on systemic security problems and longstanding failures of certain entities to fulfill individuals' rights under the Privacy Rule. The resolution agreements that OCR has entered into, as well as the single civil money penalty that we have imposed, demonstrate these priorities.

To assist providers in understanding the law and our enforcement, our outreach efforts include posting a plain language guide for health care providers on communicating with patients' family members, friends, or others involved in their care, and providing a searchable set of frequently asked questions about this topic and more.

OCR also posts a significant amount of information about our enforcement activities on our website,<sup>1</sup> which includes pages dedicated to enforcement statistics, case summaries, and detailed information about cases that have been resolved informally—through demonstrated corrective action or with a corrective action plan and settlement amount paid by a covered entity—or that have resulted in a formal enforcement action against a covered entity.

In addition, we regularly announce and emphasize our enforcement priorities through our many public speaking engagements at conferences and webinars directed to the regulated community.**Question 2:**

**As a general matter, how much discretion is left up to OCR in deciding whether to pursue penalties and corrective measures against a covered entity at all? What types of HIPAA privacy rule complaints are most likely to result in OCR taking corrective measures or imposing penalties? What guides OCR’s discretion? What factors does OCR consider?**

---

<sup>1</sup> <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html>.

The statute requires the Secretary to impose civil money penalties whenever the Department makes a formal determination that a violation has occurred, and to formally investigate those cases where our preliminary review indicates a possible violation due to willful neglect. Otherwise, the Office for Civil Rights (OCR), acting on behalf of the Secretary, retains discretion with respect to accepting cases for investigation or review, and resolving these matters informally with the covered entity, most often through the demonstrated corrective action of the entity to come into compliance. The regulatory provisions relating to HIPAA enforcement are found at 45 CFR Part 160, Subparts C, D, and E.

In the vast majority of cases, the covered entity will, through voluntary cooperation and corrective action, be able to demonstrate satisfactory compliance with its HIPAA privacy or security obligations. However, where we find indications of noncompliance due to willful neglect, or where the nature or scope of the noncompliance warrants additional enforcement action, OCR would pursue a resolution agreement with a payment of a settlement amount and an obligation to complete a corrective action plan, or would impose a civil money penalty. In addition to indications of noncompliance due to willful neglect, when deciding whether to enter into a resolution agreement with, or proceed to formal enforcement against, a covered entity, OCR would consider factors including whether the entity's noncompliance affected a very large number of individuals or resulted in demonstrated financial, physical, or reputational harm to individuals; whether the entity was noncompliant over a prolonged period of time or had failed to comply with multiple requirements of the Privacy or Security Rules; and whether the entity had a history of noncompliance or had failed to implement effective corrective actions in prior informal resolution cases.

The ultimate goal of our enforcement efforts is to protect the privacy rights of all individuals under the HIPAA Privacy and Security Rules through compliance by covered entities and business associates. Strategic use of our civil money penalty authority and high-profile resolution agreement cases draw attention to longstanding, systemic failures to comply with security or privacy requirements and raise the awareness of all covered entities and business associates of their obligations in these areas.

### **Question 3:**

**Are you concerned that the increased penalties for HIPAA privacy rule noncompliance that recently went into effect pursuant to the HITECH Act will make covered entities even more hesitant than before to share protected health information? Why or why not? Is OCR doing anything to address this preemptively?**

The purpose of higher penalties for HIPAA violations is to increase the incentive for covered entities and business associates to comply with their privacy and security obligations. Compliance involves knowing when and with whom the entity can share protected health information. As indicated above, we continue to educate covered entities and the public

regarding the ability of health care providers to share information with individuals' friends, family members, and others involved in their care.

**Question 4:**

**For which states does the HIPAA Privacy Rule prohibit state mental health facilities from submitting records for individuals who have been involuntarily committed or adjudicated as mentally defective to the National Instant Criminal Background Check System?**

On April 23, 2013, OCR issued an Advance Notice of Proposed Rulemaking (ANPRM) seeking comment from states and the public regarding barriers that HIPAA may pose to NICS reporting. Through this process, we hope to learn more about the nature and extent of any HIPAA barriers to reporting by the states. The comment period will end June 7, 2013.

As described in Question 5 below, previously, the rule did pose challenges for a New York mental health agency. New York has since changed state law, and we understand that the HIPAA Privacy Rule no longer has that effect.

**Question 5:**

**What is the nature or structure of those facilities that creates the conflict with the Privacy Rule?**

As mentioned in Question 4 above, OCR has issued an ANPRM for the purpose of learning more about the nature and extent of any HIPAA barriers to reporting by the states.

It is our understanding that in the case of New York the state mental health agency is responsible for making information regarding individuals prohibited for mental health reasons from having access to a gun available to the Federal background check system. Because the mental health agency is a HIPAA-covered entity, it previously faced some challenges to reporting the records to the NICS. Ultimately, New York State passed a statute that requires the mental health agency to report this information to the NICS, making the disclosure permissible under HIPAA as a disclosure that is "required by law." Thus, to our knowledge, HIPAA no longer prevents New York from reporting this type of information to the NICS.

**Question 6:**

**What options do the parents of a young, mentally ill, adult have if: their child's healthcare provider believes (perhaps falsely) that the HIPAA Privacy Rule prevents them from sharing information with the family, the child has refused to sign a release granting access to his health records to the parents, and a judge who has reviewed the case believes that the child has the right to refuse disclosure of his records because during a court appearance the child seemed to be of sound mind? Does HIPAA provide an exemption for such circumstances?**

A health care provider is permitted to disclose information to the family members of an adult patient who has capacity and indicates that he or she does not want the disclosure made, only to the extent that the provider perceives a serious and imminent threat to the health or safety of the individual or the public and the family members are in a position to lessen the threat. Otherwise, under HIPAA, the provider must respect the wishes of the adult individual who objects to the disclosure. However, HIPAA in no way prevents health care providers from listening to family members or other caregivers who may have concerns about the health and well-being of the individual, so the health care provider can factor that information into the individual's care.

## The Honorable Steve Scalise

### **Question 1:**

**What is the controlling factor to determine the age that a person gains Federal HIPAA rights? Is that governed by state or Federal law? Are there different standards and qualification ages for HIPAA in different states?**

HIPAA defers to state law to determine the age of majority and the rights of parents to act for a child in making health care decisions. Generally, parents or legal guardians are the personal representatives of their unemancipated minor child and can exercise the HIPAA rights of the child, including access to his or her health care record. However, there are certain exceptions, such as when state law permits the minor child to receive care without the consent of a parent or guardian and the child chooses to do so.

### **Question 2:**

**How many different institutions and medical providers have been found in violation of Federal HIPAA laws over the past 5 years? What was the amount of the fines paid in the last 5 years? By how many violators?**

From 2008 through 2012, OCR obtained corrective action from covered entities in more than 13,000 cases in which our investigations found indications of noncompliance with HIPAA.

During the same period, OCR reached resolution agreements with covered entities in 11 cases. A resolution agreement is a contract between HHS and a covered entity or business associate in which the entity agrees to perform certain obligations, make reports to HHS, and, generally, pay a resolution amount to HHS. The payments resulting from these 11 resolution agreements total approximately \$10 million.

OCR has also imposed a civil monetary penalty of about \$4 million in one case in which the covered entity failed for up to a year and a half to provide 41 individuals with access to their health information, as required by the HIPAA Privacy Rule, and failed to cooperate with OCR's investigation. OCR found the covered entity had demonstrated willful neglect (the category of noncompliance for which the highest penalties may be assessed) in its failure to cooperate, when it refused to respond to OCR's repeated demands to produce the records, failed to cooperate with OCR's investigations of the complaints, and failed to produce the records in response to OCR's subpoena, which ultimately led to a default judgment against the entity after OCR petitioned to enforce its subpoena in United States District Court.

More information about these cases, as well as other enforcement data and highlights, is available on OCR's website.<sup>2</sup>

**Question 3:**

**If a potentially suicidal patient is released to an outpatient setting from a hospital or other institution, should the doctor be required to contact the outpatient medical provider? Would it be a violation of HIPAA if they did so?**

HIPAA permits a covered health care provider to disclose information about an individual to another health care provider without the patient's authorization for treatment and coordination of care purposes, or to avert a serious and imminent threat where the second provider is in a position to lessen or avert the threat. The provider's decision whether to make such a disclosure is guided by professional ethical standards and state laws governing the practice of medicine.

**Question 4:**

**If a doctor deems an outpatient is at "high risk for suicide or other bad outcomes," is it a violation of HIPAA for the medical provider to notify the parents or consult with family members with which the patient is living? Should the doctor be mandated to notify the other family members that the patient is a "high risk for suicide or other bad outcomes," and what to watch out for at home?**

A health care provider's "duty to warn" generally is derived from and defined by standards of ethical conduct and state laws and court decisions such as *Tarasoff v. Regents of the University of California*.<sup>3</sup> HIPAA permits a covered health care provider to notify an individual's family members of a serious and imminent threat to the health or safety of the individual or the public if those family members are in a position to lessen or avert the threat. Thus, to the extent that a provider determines that there is a serious and imminent threat of an individual committing suicide, HIPAA would permit the provider to warn the appropriate person(s) of the threat, consistent with his or her professional ethical obligations and state law requirements. In addition, even where danger is not imminent, a covered provider may always communicate with individuals' family members, or others involved in the individual's care, to be on watch or ensure compliance with medication regimens, as long as the patient does not object to the disclosure.

---

<sup>2</sup> <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html>.

<sup>3</sup> [http://en.wikipedia.org/wiki/Regents\\_of\\_the\\_University\\_of\\_California](http://en.wikipedia.org/wiki/Regents_of_the_University_of_California).

## The Honorable Bill Cassidy

### Questions 1 & 2:

**Has HHS issued guidance which clearly states how a physician should handle the privacy rule when their patient is in a state of psychosis or other form of mental incapacitation? If this guidance exists, does it take into account the fact that oftentimes, an individual's disease influences them to reject the sharing of their health records, even if it is in their best interest?**

**Does OCR plan to release sub-regulatory guidance to explain—in terms that apply to medical professionals—the instances in which an individual's mental illness would constitute “incapacity”? If so, when can this guidance be expected and how will you ensure it reaches the provider level?**

Section 164.510(b)(3) of the HIPAA Privacy Rule permits covered entities, when an individual is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing information to the individual's family, friends, or others involved in the individual's care, is in the best interests of the individual.

OCR's HIPAA guidance development efforts are an ongoing and continuous process, and we intend to address as part of these efforts the issue of incapacity with respect to individuals who have serious mental illness. OCR posts its guidance on its website as it becomes available and announces the availability of new guidance to covered entities, business associates, and the public through its listserv and at public speaking events.

### Question 3:

**Panelist Carol Levine said that . . . “When family caregivers ask about their patient's care, they are routinely told ‘I can't tell you because of HIPAA.’ This is not only contrary to the law; it is not good clinical care and jeopardizes the patient's well-being.” Is there a “public friendly” federal government website that addresses these common misinterpretations and clarifies the Privacy Rule to which a family member in this situation could direct a physician or hospital administrator? If so, is there a strategy or effort to disseminate this information?**

OCR has both provider-focused and consumer-focused web-pages and plain-language guides on HIPAA and health care providers' interactions with individuals' family members and other care givers.<sup>4</sup> The consumer guide<sup>5</sup> encourages individuals to take the guide and discuss it with their health care providers and family members and other caregivers.

---

<sup>4</sup> For example, [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/provider\\_ffg.pdf](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/provider_ffg.pdf) and <http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/sharing-family-friends.pdf>.

<sup>5</sup> [http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer\\_ffg.pdf](http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer_ffg.pdf).

In addition, our YouTube channel<sup>6</sup> includes a video dedicated to this issue, which has been viewed more than 29,000 times.

**Question 4:**

**I understand that mental health and addiction Electronic Health Records (EHRs) are being shut out of state and local Health Information Exchanges (HIEs) because of aggressive federal interpretations of HIPAA and 42 CFR Part 2. As far as I know, Kentucky and Rhode Island are the only state HIEs in the nation that actually share behavioral health EHRs. Can HHS promulgate sub-regulatory guidance that will permit the sharing of behavioral health EHRs without changes to HIPAA or Part 2?**

HIEs are quickly integrating into the healthcare landscape, enabling real time access to patient health information from multiple sources. However, most HIEs currently do not have the ability to exchange behavioral health information in compliance with certain state and Federal privacy and confidentiality laws (*e.g.*, state mental health laws, 42 CFR Part 2). The Substance Abuse Confidentiality Regulations, 42 CFR Part 2, govern the use and disclosure of patient alcohol and drug abuse treatment records. These regulations establish detailed requirements for obtaining patient consent when sharing substance abuse treatment information. The exchange of behavioral health information within an HIE may be done in compliance with HIPAA without changes to the law. While it is possible for behavioral health information to be shared within an HIE without changes to Part 2, presently, most HIE systems do not have the capacity to manage the consents or to control the redisclosure of select types of information as required.

HHS has sponsored several promising projects to advance the goal of sharing behavioral health information within an HIE. These projects include: the Data Segmentation for Privacy (DS4P) Initiative, which is focused on the creation of standards to allow sensitive health information to be shared in compliance with confidentiality laws and regulations; a project, sponsored by the Substance Abuse and Mental Health Services Administration, funding five state health information exchanges (HIEs) to develop local consent policies and a common consent form compliant with 42 CFR Part 2; and an ONC-funded Behavioral Health Data Exchange Consortium, created to pilot the exchange of behavioral health medical records between providers in different states using the Nationwide Health Information Direct protocols. Additionally, through a Program Information Notice published on March, 22, 2012, ONC has already provided program guidance to state HIEs focused on assuring secure, trusted health information exchange. This guidance addresses issues related to individual choice, including offering meaningful choice and meeting the requirements of existing law. When considering the challenges of exchanging behavioral health information, it is important to also remember that state laws play a critical role. In particular, HIPAA only sets a Federal floor for privacy protections, and more stringent state laws may provide greater protections to sensitive health

---

<sup>6</sup> <http://www.youtube.com/user/USGovHHSOCR?feature=chclk>.

information and additional requirements for exchange that must be considered by state HIEs. ONC has funded work identifying and classifying these laws.

**Question 5:**

**It is the current policy of the OCR, ONC, and SAMHSA to require a patient to sign a new consent form every time a new provider joins a Health Information Exchange? In cases of serious mental illness, this is often not a practical expectation. Would HHS support, and issue guidance, that would permit a patient to opt-in or opt-out of sharing their mental health or addition Electronic Health Records (EHRs) in Health Information Exchanges (HIEs) without requiring the patient to sign a new form every time a new provider joins the HIE?**

A number of laws, both Federal and state, apply to the sharing of health records related to mental health and substance abuse treatment, including 42 CFR Part 2, which specifically relates to Federally-funded substance abuse treatment programs. Patient consent under 42 CFR Part 2 is meant to be informed, a key factor of which is the ability of the patient to know and understand – at the time of providing consent - precisely to whom he or she is giving authorization for access. Because it is impossible to anticipate future providers who may join an exchange, and equally impossible to predict future concerns a patient may have regarding his or her health record, permitting a patient to opt-in or opt-out indefinitely of having substance abuse treatment records included in an exchange may violate these important informed consent principles. SAMHSA has published two sets of frequently asked questions addressing consent and other issues.<sup>7</sup>

---

<sup>7</sup> Available at <http://www.samhsa.gov/healthPrivacy/docs/EHR-FAQs.pdf> and [http://www.samhsa.gov/about/laws/SAMHSA\\_42CFRPART2FAQIL\\_Revised.pdf](http://www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQIL_Revised.pdf).

## The Honorable G. K. Butterfield

### Question 1:

**It is my understanding that health care providers covered by the HIPAA “Privacy Rule”, must notify patients if the privacy of their health information is breached. What methods are used to notify those individuals? How does the Office for Civil Rights (OCR) ensure that health care providers are complying with the HIPAA “Privacy Rule”? What steps can individuals take if their health care record privacy has been compromised?**

Covered entities must notify affected individuals of a breach of their unsecured protected health information without unreasonable delay and in no case later than 60 days following discovery of the breach. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. The individual notification must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.

For breaches affecting more than 500 residents of a state or jurisdiction, HIPAA also requires a covered entity to notify prominent media within the state or jurisdiction.

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information by visiting the HHS website and filling out and electronically submitting a breach report form. OCR reviews and verifies the breach reports received, and, where appropriate, investigates underlying compliance issues that may have contributed to the breach and whether breach notification requirements were complied with. In accordance with a HITECH Act requirement, OCR posts information on our website about all breaches affecting 500 or more individuals. This informs the public and covered entities of specific instances of significant breaches and highlights organizational vulnerabilities that may lead to breaches of information.

Individuals may submit complaints for investigation by OCR if they are concerned that their health information has been impermissibly accessed or misused. In addition, the Federal Trade Commission (FTC) has information on its identity theft web pages about actions that individuals can take if they believe fraud was committed with their information.<sup>8</sup>

### Question 2:

---

<sup>8</sup> <http://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people>.

**If a patient objects to sharing information with certain family members or friends, is the provider able to communicate that request to other providers who may also treat the patient?**

Providers within the same legal entity or treatment setting are able to communicate regarding a patient's wishes in this regard, to ensure compliance by the covered entity with those wishes and thus, the Privacy Rule. With respect to other providers who may treat the patient, it is the right of the individual to agree or object to these other providers sharing information with his or her friends and family members.

**The Honorable John D. Dingell**

**Question 1:**

**Does current law prohibit people who are involuntarily committed to a mental institution or otherwise formally adjudicated as having a serious mental condition from owning a firearm?**

The Gun Control Act of 1968, Pub. L. 90-618, as amended, prohibits persons who have been committed to a mental institution, and individuals adjudicated by a court, board, commission, or other lawful authority as having a serious mental condition that causes them to pose a danger to themselves or others or renders them incapable of managing their own affairs, from shipping, transporting, receiving, or possessing firearms or ammunition.

The regulation, at 27 CFR 478.11, defines “committed to a mental institution” as: A formal commitment of a person to a mental institution by a court, board, commission, or other lawful authority. The term includes a commitment to a mental institution involuntarily, commitment for mental defectiveness or mental illness, as well as commitments for other reasons, such as for drug use. The term does not include a person in a mental institution for observation or a voluntary admission to a mental institution.

**Question 2:**

**Are states required to upload mental health records into NICS so individuals who are prohibited from owning a firearm do not have access to them?**

As with all of the categories of prohibited persons under the Gun Control Act, states can but are not required to make available to the NICS the identifying information for people prohibited from possessing a firearm for certain mental health reasons. Federal law encourages state reporting through various incentives, and some states have statutes requiring certain entities within the state to make this information available to the NICS.

It is important to note, however, that the NICS never has mental health records. States report only the names of ineligible individuals (among those prohibited are individuals who have been committed to a mental institution and individuals adjudicated by a court, board, commission, or other lawful authority as having a serious mental condition that causes them to pose a danger to themselves or others or being incapable of managing their own affairs) and certain other identifying information, such as their dates of birth, as well as codes identifying the submitting entity and the prohibited category that applies to the individual. The NICS system never includes information on diagnosis, treatment, or other health records.

**Question 3:**

**Current law provides for an exception to the HIPAA privacy rule for certain law enforcement purposes. Do you believe this exception permits states to report mental health records to NICS?**

No. As described below, there are other provisions that may allow for the reporting to the NICS of identifying information for people prohibited from possessing a firearm for certain mental health reasons, but the HIPAA Privacy Rule's law enforcement provisions (at 45 CFR 164.512(f)) would not permit the disclosure because the purpose of the disclosure would not be related to a specific law enforcement inquiry.

There are other Privacy Rule provisions that may apply and allow the disclosure, depending on the circumstances. Specifically, the Privacy Rule would allow the disclosure to the extent that a state has enacted a law requiring the disclosure. Alternatively, where there is no state law requiring reporting, the Privacy Rule would allow the disclosure to the extent the entity had designated itself a hybrid entity and separated its NICS reporting unit from its health care component(s), in which case the entity could report information through the non-HIPAA-covered NICS reporting unit which would not then be subject to disclosure restrictions under the Privacy Rule.

On April 23, 2013, OCR issued an ANPRM seeking comment from states and the public regarding barriers that HIPAA may pose to NICS reporting. Through this process, we hope to learn more about the nature and extent of any HIPAA barriers to reporting by the states. The comment period will end on June 7, 2013.

**Question 4:**

**Do you believe states need to pass their own laws to explicitly permit mental health reporting to NICS if the privacy rule is amended in the manner described in the Advanced Notice of Proposed Rulemaking?**

It is our understanding that some states have health information privacy restrictions in place that are more stringent than HIPAA. To the extent that is the case, if the Privacy Rule were changed to expressly permit certain covered entities to report identifying information about people prohibited from possessing a firearm for certain mental health reasons to the NICS under HIPAA, entities in some states still may face state law barriers to reporting such information. We hope to learn more from public feedback we receive in response to our Advance Notice of Proposed Rulemaking (ANPRM) on HIPAA and NICS reporting, in which we requested comments on any HIPAA and non-HIPAA barriers states face in reporting certain information to the NICS. The comment period will end June 7, 2013.