KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **Deven McGraw**
Director, Health Privacy Project
Center for Democracy & Technology

Before the U.S. House Committee on Energy & Commerce
Subcommittee on Oversight & Investigations

Does HIPAA Help or Hinder Patient Care and Public Safety?

April 26, 2013

Chairman Murphy and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today.

The Center for Democracy and Technology ("CDT") is a non-profit Internet and technology advocacy organization that promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education, and litigation, as well as through the development of industry best practices and technology standards. Recognizing that a networked health care system can lead to improved health care quality, reduced costs, and empowered consumers, CDT is using its experience to shape balanced, workable privacy solutions for a health care system characterized by electronic health information exchange.

The question posed at this hearing is whether the privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) help or hinder patient care and public safety. The short answer is that HIPAA's provisions by design enable the sharing of health information, including mental health information, for both patient care and public health and safety. However, frequently these provisions are not fully understood and are too often misinterpreted, which may have a detrimental impact on both policy goals.

Privacy is Fundamental to Good Health Care

Americans consistently express concerns about the privacy of their health information. Researchers have focused on this issue more intensively in the last several years in response to initiatives aimed at increasing adoption of electronic health records. In a 2006 survey, when Americans were asked about the benefits of and concerns about electronic health records:

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 55% were concerned about insurers gaining access to this information.[1]

Privacy rules are frequently criticized as providing obstacles to effective care, but in fact the opposite is true: patients who mistrust whether their information will be handled confidentially will not fully participate in their own health care.[2] Without appropriate protections for privacy and security in the healthcare system, people will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[3] Such privacy-protective behaviors include failing to seek care for sensitive medical conditions, asking health care providers to leave sensitive information out of the medical record, and traveling outside of the area to seek care.[4] According to a 2007 poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical

[1] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006). In a more recent survey conducted by the Markle Foundation, more than 80% of both the public and doctors surveyed said that requiring protections and safeguards for patient privacy was important. http://www.markle.org/publications/1443-public-and-doctors-agree-importance-specific-privacy-protections-health-it (January 2011)

[2] See Janlori Goldman, "Protecting Privacy to Improve Health Care," Health Affairs (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), http://www.chcf.org/topics/view.cfm?itemID=12502 (Promoting Health/Protecting Privacy).

[3] Id.

[4] Id.

data might be disclosed.[5] A September 2011 study by the New London Consulting commissioned by FairWarning®, a vendor of breach detection software, found that:

- 27.1% of respondents stated they would withhold information from their care provider based on privacy concerns.
- 27.6% said they would postpone seeking care for a sensitive medical condition due to privacy concerns.
- Greater than 1 out of 2 persons said they would seek care outside of their community due to privacy concerns, and 35% said they would drive more than 50 miles to seek care.[6]

The consequences of this climate of fear are significant – for the individual, for the medical community, and for public health and safety:

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to or impact others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[7]

Assurances of confidentiality are particularly important for mental health treatment. It is estimated that one in four adults in America suffers from a diagnosable mental disorder in a given year; [8] nearly 2/3 do not seek treatment due in part to lack of knowledge, fear of disclosure, potential rejection of friends, and discrimination.[9] Laws protecting mental health information are designed to help address these fears and remove potential barriers to treatment.

---

[5] Harris Interactive Poll #27, March 2007. Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors. National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005).

[6] http://www.fairwarningaudit.com/documents/2011-WHITEPAPER-US-PATIENT-SURVEY.pdf

[7] Protecting Privacy, supra note 2.

[8] NIMH – The Numbers Count: Mental Disorders in America, http://www.nimh.nih.gov/health/publications/the-numbers-count-mental-disorders-in-america/index.shtml.

[9] "Facts about Stigma and Mental Illness in Diverse Communities," National Alliance on Mental Illness, http://www.nami.org/Content/Microsites270/NAMI_Howard_County/Home258/Multicultural_Action1/StigmaandMentalIllnessinDiverseCommunities.pdf.

Protections and Permissions for Using and/or Disclosing Health Information

The HIPAA Privacy Rule sets parameters for the use and disclosure of identifiable health information by health care providers, health plans, and health care clearinghouses, and the contractors (or business associates) who obtain identifiable health information in order to perform services on their behalf. The Privacy Rule takes a decidedly balanced approach to privacy, giving individuals the right to control certain uses and disclosures while also expressly allowing uses and disclosures to meet routine health care needs and public policy goals. In general, the Privacy Rule requires the express authorization of the patient before identifiable health information can be accessed, used or shared, but the Rule includes a number of exceptions designed to facilitate access and sharing of health information for patient care, to facilitate payment for care, for public health, and for other uses deemed critical to a functioning health care system. Of particular importance to this hearing, the Privacy Rule allows a patient's health information to be shared to facilitate treatment, without the need to obtain either an oral consent or formal written authorization from the patient.

The Privacy Rule treats all identifiable health information the same, with one notable exception: psychotherapy notes are provided with additional protections. Not all mental health information about a patient qualifies as "psychotherapy notes;" that term is limited to the notes of a mental health professional taken during a counseling or therapy session.[10] Entities covered by the Privacy Rule must obtain a specific, formal authorization from the patient in order to disclose psychotherapy notes in most circumstances (such notes can be used internally to treat the patient).[11] In addition, the right of patients to access and obtain a copy of their health information does not apply to psychotherapy notes.[12]

---

[10] Psychotherapy notes are "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record. The term 'psychotherapy notes' excludes data relating to medication prescription and monitoring, counseling session starts and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." 45 C.F.R. 164.501.

[11] 45 C.F.R. 164.508(a)(2). Such notes may be used by the originator in order to treat the patient; they also can be used for training purposes and to defend against a legal action or other proceeding. Id. Of note, the U.S. Supreme Court, in a case recognizing psychotherapist-patient privilege in federal rules of evidence, acknowledged the critical role that confidentiality of psychotherapy notes plays in mental health treatment: "Effective psychotherapy … depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals consult psychotherapists, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment." Jaffree v. Redmond, 518 U.S. 1 (1996).

[12] 45 C.F.R. 164.524(a)(1)(i).

The Privacy Rule also includes a number of provisions that expressly allow certain uses and disclosures of health information for important public policy reasons. These exceptions allow entities covered by HIPAA to use or disclose information: when required to by law; for public health activities; for the reporting of abuse; for health care oversight; for judicial and administrative proceedings; for law enforcement; and to coroners, to note just a few examples.[13]

Of specific interest for this hearing, entities covered by HIPAA are expressly permitted to use or disclose information to avert a serious threat to health or safety. Specifically, an entity may,

> "consistent with applicable law and standards of ethical conduct, use or disclose protected health information if [it], in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and [the use or disclosure] is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat."[14]

Entities are expressly presumed to be acting in good faith if they are acting based on actual knowledge "or in reliance on a credible representation by a person with apparent knowledge or authority."[15] On January 15, 2013, the HHS Office for Civil Rights issued a two-page, to-the-point letter to health care providers alerting them to this exception, in the hope of dispelling widespread myths that HIPAA does not permit such disclosures.[16]

The HIPAA Privacy Rule provides a floor of privacy protections, at least for health data collected, used and shared by entities covered by its provisions. However, it is not the only law protecting mental health data. States are permitted to enact more stringent protections for health privacy, and nearly all states have specific statutes related to mental health privacy.[17] In addition, Congress has expressly acted to protect the privacy of health information in other sensitive records, and these laws were not preempted by HIPAA. In recognition of the potential stigma and the legal implications of seeking alcohol and drug treatment, Congress enacted the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law, which provides heightened protections for alcohol and drug use treatment records maintained by any programs receiving some

---

[13] See provisions of 45 C.F.R. 164.512.

[14] 45 C.F.R. 512(j). This provision also includes the circumstances under which law enforcement can be alerted when an individual has admitted committing a violent crime or is believed to have escaped from a correctional institution or from lawful custody. 45 C.F.R. 512(j)(1)(ii).

[15] 45 C.F.R. 512(j)(4).

[16] http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/righttoaccessmemo.pdf.

[17] Beckerman, J et al., "Health Information Privacy, Patient Safety, and Health Care Quality: Issues and challenges in the Context of Treatment for Mental Health and Substance Abuse," BNA's Health Care Policy Report, vol. 16, No. 2 (January 14, 2008). This article includes a comprehensive discussion of HIPAA's provisions regarding "preemption."

form of federal assistance.[18] The Family and Educational Rights and Privacy Act of 1974 (FERPA) protects the privacy of student education records, including information related to treatment of a student for substance use or mental health conditions.[19] Most state laws restricting disclosures of health information typically include emergency exceptions;[20] however, we are not aware of any comprehensive compilations of state mental health laws (such state law surveys are typically expensive to produce and rapidly rendered out of date) that would enable us to discuss state law provisions in more detail. FERPA includes an exemption allowing disclosure of student information in emergencies, when the information is necessary to protect the health or safety of the student or others.[21] Regulations governing federally assisted alcohol and drug treatment programs have more limited exceptions for emergencies.[22]

Ability to Share Health Information with Family, Friends under HIPAA

When HIPAA's Privacy Rule first went into effect a decade ago, people widely believed that it did not permit disclosure of a patient's health information to family members under any circumstances. That has never been the case, but this myth stubbornly persists. The Privacy Rule expressly permits disclosure to someone who is involved in a patient's care or in payment for that care -- either a family member, other relative, or a close personal friend of the patient, or any other person identified by the patient -- unless the patient objects to the sharing of that information.[23] The information that may be shared is only information that the person involved in the patient's care (or in paying for that care) needs to know (so past diagnoses not related to the patient's current health condition, for example, could not be shared under these provisions). If the patient is not conscious (or not present), a provider can still share relevant health information with family or friends if he or she believes it is in the patient's best interest to do so.

The HHS Office for Civil Rights has issued guidance on these provisions, which explains them more clearly and in non-legal language;[24] however, it is unclear how

---

[18] Id. See 42 C.F.R. Part 2 for the regulations that set forth the stringent rules regarding use and disclosure of patient information.

[19] Id. See 34 C.F.R. Part 9 for regulations.

[20] Id.

[21] Id. See 20 U.S.C. 1232g.

[22] 42 C.F.R. Part 2 permits disclosure of information without consent to enable notification of medical personnel in the event of a medical emergency (in a situation that poses an immediate threat to the health of any individual); to enable notification of law enforcement if an immediate threat to health or safety of an individual exists due to a crime on program premises or against program personnel; and to enable reporting under state law of suspected child abuse or neglect. Information can be disclosed to law enforcement about an immediate threat to the health or safety of an individual not involving a crime on program premises or against program personnel if patient-identifying information is not disclosed. http://www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQII_Revised.pdf.

[23] 45 C.F.R. 510(b).

[24] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf.

many providers, individuals, and family members are aware of this guidance. This guidance also may not be in sufficient detail to address common questions and clear misperceptions.

HIPAA requires that a patient's "personal representative" be treated as the patient for purposes of the Privacy Rule.[25] Persons who, under applicable law, have authority to act on behalf of a patient for health care decision purposes must be treated as personal representatives. For minors, this typically is a parent, guardian or other person acting *in loco parentis*; however, where state law permits the minor to seek care without the consent of a parent, which in some states may be the case for mental health treatment, the minor has greater authority to designate when a parent or guardian can receive health information. State laws typically establish the circumstances under which an individual may act as the personal representative of another with respect to health care decisions.

Paths Forward

As noted above, the HIPAA Privacy Rule permits the sharing of relevant mental health and other personal health information in order to avert a serious threat to health or safety, and to family members and friends who are involved in a patient's care, with some exceptions. It is important to keep in mind, however, that the Privacy Rule *permits but does not require* information to be shared in these circumstances. (The Privacy Rule only expressly requires information to be shared in two instances: (1) with the patient or his or her personal representative, or (2) with the government in the event of a HIPAA compliance audit.)

Fear of liability for violating HIPAA's provisions, coupled with misunderstanding of its provisions, can be a recipe for not sharing, even in circumstances where such sharing is expressly permitted and arguably important for patient care and/or public safety. Additional guidance from the Office for Civil Rights, with even greater clarity on permitted uses and disclosures, could be enormously helpful at dispelling myths and easing the concerns of mental health professionals. Working with relevant professional societies to ensure that this guidance is widely disseminated (and written in terminology likely to be understood) would also be helpful. The Administration should also take steps to ensure such guidance can be issued in a timely way.

States should also examine their statutes covering mental health information to ensure that they meet the needs of patients both for confidentiality and to have the wanted support of family and close friends in their care, and urgent public safety needs.

[25] 45 C.F.R. 164.502(g).

Conclusion

Thank you for the opportunity to present this testimony, and I would be pleased to answer any questions you may have.