TESTIMONY OF MARK A. ROTHSTEIN, J.D.

UNIVERSITY OF LOUISVILLE SCHOOL OF MEDICINE

Before the

SUBCOMMITTEE ON PRIVACY, CONFIDENTIALITY, AND SECURITY

NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

Strengthening the Minimum Necessary Standard

June 16, 2016

My name is Mark Rothstein, and I am the Herbert F. Boehl Chair of Law and Medicine and Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. From 1999-2008, I was a member of the NCVHS, and I had the privilege of chairing what was then called the Subcommittee on Privacy and Confidentiality.

I want to thank the subcommittee and staff for inviting me to testify this morning about the minimum necessary standard. I believe that minimum necessary is one of the most important concepts in the HIPAA Privacy Rule. As I will further describe, I also believe that this provision needs to be better defined, explained, studied, expanded, and enforced.

I. Why minimum necessary is so important

As most people in this room are well aware, the Privacy Rule provides only limited rights and protections for individuals whose health information is used and disclosed by covered entities. In most cases, individuals have virtually no control over whether their protected health information (PHI) is used and disclosed. Under the Privacy Rule, no consent or authorization is necessary for a covered entity or business associate to use and disclose PHI for treatment, payment, and health care operations. Instead, covered entities are merely required to provide a notice of privacy practices and, where there is a direct treatment relationship, to make a good faith effort to obtain an acknowledgement from the individual that he or she has received the notice.

In my view, the notice and acknowledgment approach is seriously deficient and, on balance, is detrimental to the Privacy Rule. Most patients do not get a copy of the notice and those who do often do not understand it. I think the process has come to symbolize the Privacy Rule as an arcane formality with no discernible, positive effect on their health privacy.

Another limitation of the Privacy Rule is that disclosures for 12 categories of public purposes do not require consent or authorization. The broadly-worded exemptions apply to disclosures: (1) required by law; (2) public health activities; (3) abuse, neglect, or domestic violence; (4) health oversight activities; (5) judicial and administrative proceedings; (6) law enforcement purposes; (7) decedents; (8) cadaveric organ, eye, or tissue donation; (9) some research uses; (10) to avert a serious threat to health or safety; (11) for specialized government functions, including national security; and (12) workers' compensation. It should be mentioned that the minimum necessary standard applies to all of these disclosures except for those required by law. 45 C.F.R. § 164.502(b)(2)(v). Because it is largely unknown whether the minimum necessary requirement is actually followed for the 11 other types of disclosures, HHS-supported research would be extremely helpful in quantifying the rates of compliance, thereby indicating whether additional regulatory, education, or enforcement action is needed.

After adding the 12 public purpose exceptions to treatment, payment and health care operations, there are only three main categories of uses and disclosures left: fundraising, marketing, and research. The fundraising provision was amended in 2013 to permit disclosure of date of service information, physician information, and outcome information. Marketing was left largely unchanged in 2013, and still requires an authorization before disclosing PHI for marketing. As for research, there have been efforts in Congress to eliminate some of the Privacy Rule's protections for research, such as permitting covered entities to sell PHI to researchers. If these

measures are enacted, this would weaken one of the last areas where the Privacy Rule has meaningful protections.

Because the Privacy Rule does not protect whether an individual's health information is used and disclosed, to have any value it must regulate the amount of health information disclosed and the form in which it is disclosed. That is where "minimum necessary" comes in and why it is so important. The minimum necessary provision reads: "When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." 45 C.F.R. § 164.502(b)(1).

Although this is an extremely valuable provision, my sense is that it is not well understood. I believe that HHS should undertake educational efforts to ensure that minimum necessary is comprehended by individuals and implemented by covered entities.

II. Why minimum necessary needs to be extended to treatment

The minimum necessary rule currently applies to payment and health care operations, but not treatment. 45 C.F.R. § 164.502(b)(2)(i). Therefore, any health care provider, not merely any physician, customarily has the ability to access a patient's entire health record for any treatment purpose. Many health care institutions have adopted "role based access" measures, which limit access of staff members based on their role. For example, a hospital's food service staff would have access only to a patient's dietary information.

Another widely used measure, audit trails, document access to a patient's health information by health care providers. Audit trails serve to discourage personnel from unauthorized access to PHI, such as viewing the records of individuals who are not their patients, including relatives and celebrities being treated at the institution.

Neither role based access controls nor audit trails prevent or discourage authorized health care personnel from viewing a patient's entire medical record when the patient is being seen for a discrete health problem and there is no medical reason for unlimited review of the patient's record. As I will further describe, this is where "minimum necessary" could be very helpful.

When the Privacy Rule was drafted, our health record system was largely paper based and decentralized. The inadequacies and inefficiencies of paper records are well known, but such a chaotic system was ideal for protecting privacy because it was impossible for anyone, including the patient, to obtain old records created or maintained by numerous, unaffiliated, prior health care providers. Old sensitive information, such as a decades old record of domestic abuse, reproductive conditions, mental illness, substance abuse, or similar information was, literally, unavailable. By contrast, today's electronic health records (EHRs) are designed to be comprehensive and longitudinal, increasingly covering all health care encounters from birth to the present. Furthermore, consolidation in the health care industry has accomplished what the lack of interoperability prevents -- easy access to inclusive health information. EHRs are

potentially a vast improvement over paper records in terms of efficiency and quality, but it is important to make protecting privacy a part of their design and operation.

For many years, and in several letters to the Secretary, the NCVHS has recognized the privacy risk of sensitive information with no current clinical utility being routinely accessible by all health care providers. That means sensitive information recorded in the past by one provider, such as a psychiatrist, urologist, or obstetrician-gynecologist, is accessible now – and in the future -- by all other health care providers in integrated practices or when PHI is sent to another provider for a consultation. For example, a patient seeking emergency room care for a sprained ankle should be confident that his or her reproductive health information will not be viewed, but that confidence would be misplaced today.

Let me be clear. The overwhelming majority of health care providers have neither the time nor inclination to troll through voluminous records to search for sensitive information, but the mere fact that they could is very unsettling to many patients. Patients would be greatly distressed to realize that their most sensitive health secrets will always be only a click away from disclosure.

It is also important to recognize that the lack of protection for sensitive health information affects all of us – not just individuals with sensitive information in their EHRs. Concern for privacy is a leading reason why individuals with mental illness, substance abuse, infectious diseases, and similar conditions delay or forego treatment. Thus, ensuring privacy is important to all of our health and safety.

The NCVHS has recommended that individuals should be able to segment their PHI by excluding from routine access certain predetermined categories of sensitive information in an EHR. Amending the minimum necessary rule to apply to treatment would be an effective way of implementing these prior recommendations.[1]

III. Why uses and disclosures for payment and health care operations ought to be in the "least identifiable form"

Many breaches of privacy occur in claims processing (under "payment") and administrative functions (under "health care operations"). In preparing and submitting a claim, evaluating the claim, and processing it, an individual's PHI may be viewed by 100 or more individuals. There is no reason why, at this point, the information needs to be in individually-identifiable form. For example, the billing department at a hospital and the payment department at a health insurer only need to know that certain covered services were provided to Patient 1234, who is covered under Health Plan XYZ. If there is a problem, then the code can be broken to learn the identity of the individual. Similarly, in conducting health care operations, such as reviewing patient records for quality assurance purposes, it does not matter who the patient was. It only matters what services were provided, by what providers, when, what the outcome was, etc.

[1] See J.L. Agris, Extending the Minimum Necessary Standard to Uses and Disclosures for Treatment, *Journal of Law, Med. & Ethics* 43(1) (2014): 263-267.

It would be relatively easy to convert from names-based billing to the use of a unique billing code, and doing so would greatly advance the privacy of individuals. The number would not be a national patient identifier, but a number assigned by a health insurer, such as the "member" number on a patient's health insurance card, which already exists.

In addition, removing patient names before using PHI for health care operations is feasible and would significantly increase privacy. To clarify, I am not recommending compliance with the detailed deidentification provisions of the Privacy Rule (45 C.F.R. § 164.514(b)). I am merely advocating that names be replaced with a number for payment and health care operations.

Conclusion

I recall a hearing of this Subcommittee many years ago in rural Utah, as part of a series of hearings about the Privacy Rule we conducted around the country. One of the witnesses told us that disclosing identifiable health information beyond the doctor's office invariably meant that everyone in the small town would learn about an individual's sensitive health information. Many of us on the Subcommittee did not realize that in a small town the usually anonymous people working in the payment chain are a patient's neighbors, relatives, and friends. This example illustrates why HHS needs to ensure that PHI used or disclosed in any community and for any purpose is protected to the greatest extent reasonably possible.

I respectfully propose that the NCVHS recommend to the Secretary that the minimum necessary standard be extended to treatment. In addition, a "least identifiable form" requirement should be applied to payment and health care operations. I believe these amendments would be extremely valuable in their own right, and they would also enhance the legitimacy of the HIPAA Privacy Rule.[2]

[2] See M.A. Rothstein, The End of the HIPAA Privacy Rule? *Journal of Law, Med. & Ethics* 44(2) (2016): 352-357.