ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **bob@bobgellman.com**
Washington, DC 20003 **www.bobgellman.com**

June 16, 2016

Summary of Testimony on Strengthening the Minimum Necessary Standard
Subcommittee on Privacy, Confidentiality, and Security, National Committee on Vital and Health Statistics

Main Point: HIPAA allows many non-consensual uses and disclosures. The minimum necessary rule is an important component of controlling those uses and disclosures.

1. The minimum necessary rule is important for privacy. The general privacy policy principle is that all processing of personal data should be allowed for defined purposes and limited as much as possible. Any processing of personal information affects privacy and needs a sufficient justification. Health records are large, have much personal information, and pass through many hands. The minimum necessary rule is an important general constraint. The Committee should reaffirm the importance of the rule.

2. Under the Privacy Rule, disclosures for law enforcement and national security are especially broad and lack adequate standards and appropriate procedures. Allowable nonconsensual disclosures for public health, health oversight, organ donation, research, specialized government functions, and others are somewhat less troublesome, but all could stand to have stricter controls as well. The minimum necessary rule is important because it applies to these disclosures and obliges a covered entity to pay more attention when it makes non-consensual disclosures for purposes not directly related to health care treatment and payment.

3. When a covered entity discloses a health record to a third party who is not a HIPAA covered entity, the record generally passes beyond the limits of HIPAA. A disclosed HIPAA record may be subject to no privacy restriction at all in the hands of the recipient. The minimum necessary rule limits both disclosure and the consequences of disclosure outside the HIPAA umbrella. This is an additional reason the minimum necessary rule is essential.

4. The exception from minimum necessary for treatment disclosures is probably still an unfortunate necessity at the present time. We need to begin to prepare the health industry for a transition to a narrower rule. As health records continue to expand into lifetime records, there will be parts of that record that a patient will not want shared with future providers. I am not suggesting that patients should have full control, but reasonable patient interests in confidentiality should be accommodated.

5. With respect to controlling parts of records when disclosed for treatment, I recognize that the notion of special rules for so-called sensitive information is attractive. Sensitive information is a troubled concept, and I advise against relying on fixed categories of sensitive information. One individual's sensitive information is another individual's cocktail party chatter. Patients can be offered menus that allow they to identify what is sensitive to them, recognizing that individual preferences will change over time. Protecting information, especially in a treatment context, will require some tradeoffs.

6. In addition to providing current guidance, the Committee should recommend that the Secretary issue additional guidance telling covered entities that the current minimum necessary rule blanket exception for treatment is likely to change in the future and that covered entities should start preparing for a shrinking exception by demanding technology that will help comply with a narrower exception for treatment disclosures. The same guidance will inform health information technology companies of the need to develop new software. Technology rather than formal regulation may also help limit uses and disclosures for payment and operations.

7. Areas that minimum necessary guidance should address include: law enforcement, national security, public health, research, and fundraising. Activities that affect the processing of large numbers of records should receive priority in guidance. Here are a few additional issues that could stand some clarification. The references to FAQs are to those on the HHS website.

a. I do not understand some of the current exemptions to minimum necessary. One exemption covers disclosures pursuant to authorization. If I authorize disclosure of PHI from my last doctor visit, the exemption suggests that it is okay to disclose all of my records and not just what the authorization expressly covers. FAQ 210 provides a better gloss, saying that a covered entity can disclose what is requested on the authorization. However, the rule itself is not as clear as it should be.

Another exemption from minimum necessary covers disclosures required by law. If a law requires disclosure of a communicable disease to a public health authority, does the exemption mean that a covered entity can disclose psychotherapy notes not addressed in the law? If these disclosures are routine and recurring, are they also exempt from the provision about suing standard protocols [§ 514(d)(3)(i)] ?

The problem with the rule in both cases is that the exemption is stated too broadly. The issue is not whether a disclosure should be limited to the minimum necessary to accomplish a request, but it is whether a covered entity has to assess the intended purpose of the disclosure. I suggest that these are two different activities in many cases. Until the rule can be adjusted, this is a point that should be clarified in guidance. I do not think that FAQ 210 is sufficient as written.

b. FAQ 215 says that facility redesigns are not necessary to meet the reasonableness standard for minimum necessary uses. In the short term, that is a fair policy. But in the long term, the perspective is too narrow. I am not mandating retrofits for existing technology, but much can be done with new technology if the requirements are clear and if there is sufficient lead time for implementation. The next generation of technology can often do better without major additional cost. Further, at least some of the old FAQs on minimum necessary (and otherwise) continue to reflect the paper records environment from two decades ago. Some revisions would be appropriate for the EHR era.

c. FAQ 217 says that a covered entity can rely on an institutional review board's determination that the information requested by a researcher is the minimum necessary for the research purpose. I have no evidence to offer here, but I have my doubts that IRBs (or researchers) uniformly understand and apply the minimum necessary rule uniformly. I would like to see guidance that says that a covered entity has the ability to make its own determination about minimum necessary if it chooses to do so.

I make the same point about representations from public officials that the provision in § 514(d)(4)(iii)(A) allows. Does anyone really think that a public official making a request/demand pays much attention to minimum necessary standards? There is at least some basis for relying on a request from a covered entity that arguably understands the Privacy Rule, but that basis is mostly absent from official requests.

*****