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

Statement of Robert Gellman
Privacy and Information Policy Consultant

HIT Policy Committee

September 18, 2009

Thank you for the invitation to participate in this meeting. I am a privacy and information policy consultant in Washington, DC. I served for 17 years as a staff member in the House of Representatives, with broad responsibilities for privacy and information policy matters. I drafted several health privacy bills that moved part way through the legislative process but never became law. I served as a member of the Department of Health and Human Service's National Committee on Vital and Health Statistics (1996-2000). I am a graduate of the Yale Law School.

I have written extensively on privacy and health privacy matters. Many of my papers are available at http://www.bobgellman.com. A recent publication of relevance here is *Notes and Observations on Selected Parts of Title XIII, Subtitle D, Privacy, American Recovery and Reinvestment Act Of 2009*, available at http://bobgellman.com/rg-docs/Stimulus-Privacy-HIPAA-Analysis.pdf.

Recent publications for the World Privacy Forum expressly on health privacy include: *Personal Health Records: Why Many PHRs Threaten Privacy* (together with a consumer advisory) available at http://www.worldprivacyforum.org/personal_health_records.html; *Patient's Guide to HIPAA*, available at http://www.worldprivacyforum.org/hipaa/index.html; Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, available at http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf; and FAQs for Victims of Medical Identity Theft, available at http://www.worldprivacyforum.org/FAQ_medicalrecordprivacy.html. There is also a somewhat related paper on *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, available at http://www.worldprivacyforum.org/cloudprivacy.html.

The Committee asked me to address accounting for disclosures, audit logs, and transparency (e.g., privacy notices, changes to privacy policies, notifications, privacy after mergers and bankruptcies, etc.). I discuss the accounting and audit logs as a unit. I then offer a few comments on transparency, followed by comments on some other issues that are also on today's agenda.

Accounting for Disclosures

1. Uses and Disclosures Should Be Covered

In any fully computerized system of health information, it is essential that there be accounting records for all uses and disclosures. **I emphasize that accounting should include internal uses as well as external disclosures.** In the HIPAA regulations, HHS erred by not mandating accounting for all disclosures (current exceptions include disclosures for treatment, payment, and health care operations) and for all uses. Any modern computer system will maintain an accounting for use and disclosure activity as a means of internal control. I do not support accounting requirements for internal uses of paper records or for spoken communications. Requiring accounting in those areas is too expensive or too cumbersome.

I note that the issue of accounting for disclosures made for treatment, payment, and health care operations for EHR has been partially cured in Title XIII of the American Recovery and Reinvestment Act of 2009. Section 13405(c)(1)(A) provides that the regulatory exemption for treatment, payment, and health care operations does not apply to EHRs. The legislation solves part of the problem, **but it does not cover uses**. That remains a huge loophole.

I observe that some of the problems of medical identity theft result from the misuse of health records by insiders. For example, some hospital personnel copy parts of patient records and sell them to confederates who engage in fraudulent billing, financial identity theft, and other crimes. Automated accounting records may be the best method for discouraging this type of crime or for holding people accountable for it. The constant stream of stories about snooping in the files of celebrities by hospital employees is **compelling evidence about the need to account for uses as well as disclosures.** Snooping for medical identity theft purposes rarely gets the same attention, but it may be the bigger problem.

See the World Privacy Forum's pioneering report: *Medical Identity Theft: The Information Crime that Can Kill You*¸ available at http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

2. Time Limits for Accounting Access.

In Section 13405(c)(1)(B), ARRA also changed the requirement for patient access to accounting records from six years in the HIPAA rule to three years, a period that is much too short. Covered entities will likely maintain accounting data for much longer periods, if not forever. **If accounting records exist, a patient should have a right to have a copy.** I urge the Committee to ask Congress to extend the three-year period or to ask HHS to provide an express right of access to all existing and readily retrievable accounting records, whether or not maintenance of the records is mandated by law.

3. Amount of Time for Compliance

In the HIPAA regulation, HHS should have allowed more time for covered entities to comply with the accounting requirements. **Any new requirement should be prospective so that it only**

applies to new computer systems placed in service at some time in the future. If record keepers have sufficient notice of the requirement, it will be relatively easy to include the capability for audit trails for both uses and disclosures at little additional cost in any EHR system. I suggest that the requirement be phased in. Those who have the capability of complying must do so on the effective date of the regulation. Those who have partial capability must do what they can on the effective date. Those who do not have the capability to comply with an expanded accounting requirement should be told to comply when their systems develop the capability to do accounting or when their next generation of software comes on stream, which ever comes first. I suggest that an absolute time limit for full compliance be set at ten years. Accounting is relatively easy to do as long as you do not have to retrofit an existing computer system.

4. Accounting for Consensual Disclosures

Another problem with the HIPAA rule is that there is no accounting required for consensual disclosures. This is a major mistake. With PHRs coming into broader use, there will be more disclosure of health records outside the regulated health care system. **Patients may never remember that they gave consent to the disclosure of their health care records** when they checked (or perhaps failed to uncheck) a box on a website that they visited years earlier. Without accounting records, there may be no trace of these activities anywhere. It is possible that some action taken by an unaware patient could result in sharing of lifetime health records with a profiler or marketer, with a covered entity's accounting record the only possible way that the patient may ever learn of the sharing.

5. Require a Court Order to Suspend Law Enforcement or Health Oversight Requests

The HIPAA rule [(§ 164.528(a)(2)] allows for a temporary suspension of an individual's right to receive an accounting of disclosures to a law enforcement official or to a health oversight agency. This is poor policy. The rule allows a requester to offer a 27th generation photocopy of a boilerplate demand for accounting suspension. **If there is an adequate reason for suspension, the rule should require a court order to suspend accounting.** Obtaining a court order will establish a sufficiently high procedural barrier so that exclusions will not be sought casually. In the alternative, if a simple written request for exclusion is acceptable, the request should be dated, signed by supervisory official, and contain a certification that the official is personally familiar with the purpose of the request and the justification for exclusion from accounting.

6. What Information Belongs in an Accounting Record?

Section 13405(c)(2) directs the Secretary to issue regulation on what information should be collected about each disclosure. The law appropriately identifies the elements that should be considered by the Secretary in making choices. Administrative burden is a reasonable concern. However, **the burden of creating an accounting record for an EHR is minor**. A computer can be programmed to record as much or as little information as is desired. Storage of information is extraordinary inexpensive today, and cost of storage should not be a factor. The question is what would be useful to individuals. **The answer is that an accounting record**

should show the date, identity of recipient, and, in most cases, purpose. For external disclosures, it may be appropriate to identify institutional recipients rather than named individuals. For internal uses, the name and job title of recipients should be included. Ideally, the record (or a readily available guide) should contain enough information to tell a patient why each recipient looked at the patient's record.

Accounting for disclosures should include not only the actual recipient. **The accounting record should also identify actual party in interest** whenever possible. This is essential in any disclosures made for marketing (whether consensual or otherwise). For example, if a pharmacy disclosed patient data to a lettershop for a marketing campaign funded by a drug manufacturer, the accounting should identify both the lettershop and the manufacturer. Telling the patient that the XYZ Lettershop received the data is not as meaningful as telling the patient that the ABC Pharmaceutical Company benefited from the disclosure. This type of detail will be essential as more third parties (e.g., PHRs) seek records from covered entities. **If the real party in interest is not identified, then some will hide their activities behind obscure and untraceable intermediaries**.

I note that § 13405(e)(1) requires a covered entity to *transmit such copy directly to an entity or person designated by the individual*. While there is a good purpose here, this requirement could be easily abused by a marketer who exploits an unknowing patient. Suppose that a health record disclosure authorization is included as one of a dozen forms a consumer must complete to obtain a mortgage, enroll in college, register a new PC, or some other complex activity. Without an accounting record for the "consensual" disclosure, that consumer's record could be disclosed for years without any trace (unless a covered entity is allowed to ask if the patient *really* meant to share that patient's lifetime health record with the Shady Marketing Company).

7. Accounting and Business Associates

Section 13405(c)(3) provides a new and very convoluted provision for accounting for disclosures by business associates. I quote the language here for convenience.

> (3) PROCESS.--In response to an request from an individual for an accounting, a covered entity shall elect to provide either an--
>
> (A) accounting, as specified under paragraph (1), for disclosures of protected health information that are made by such covered entity and by a business associate acting on behalf of the covered entity; or
>
> (B) accounting, as specified under paragraph (1), for disclosures that are made by such covered entity and provide a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address).
>
> A business associate included on a list under subparagraph (B) shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting.

This provision is poorly considered, unfair to patients, and should not have been included in a statute. I assume that its presence is the result of industry complaints about the current accounting rule. If that is indeed the case, it illustrates that coming to Capitol Hill for a solution to problems often results in worse problems, especially when statutes are drafted in the middle of the night.

The new provision allows a covered entity to provide a complete accounting to a patient that includes all disclosures made by the covered entity and its business associates. That's fine. However, in the alternative, **it allows a covered entity to reveal only its own disclosures and to provide the requesting patient with a list of names and addresses of business associates. The patient would then have to make a request of each business associate separately.** This is worse than useless. It imposes costs for the maintenance of accounting records on business associates that patients will almost never be able to find or use.

Since a large hospital may have dozens or even hundreds of business associates, the requirement that each patient make separate requests of business associates could be enormously expensive to all involved. Business associates may be in other countries or may have no reason to be responsive to patients.

One limiting factor may be the unwillingness of some covered entities to reveal the number or identity of their business associates. A hospital may not want to tell patients that it employs the Type-By-Night transcription service in a third world country. Indeed, a list of business associates for a large health care institution could be valuable to competitors by revealing confidential relationships.

Does the ability to "pass the accounting buck" to business associates apply to business associates themselves? If so, each business associate could give a requesting patient a list of its own disclosures plus a list of its business associates. The tree of business associates from a single covered entity to dozens of primary business associates to numerous second-degree business associates and then third and fourth degree business associates could encompass hundreds or thousands of entities throughout the world. Each business associate has its own lawyers, accountants, computer providers, and others that would also be subject to accounting. At some point, there has to be an end to the process that will not support evasion of the basic requirement.

A simple request by a patient seeking to find the source of a specific improper disclosure could require much effort and significant cost for the patient. It could take hours and hours to follow the chain of business associates and make seriatim requests. Most patients would effectively be unable or unable to use the accounting provision under those circumstances. If even a few patients persist with requests throughout the chain of business associates, the costs imposed on all will be significant. Further, tracing accountings through chains of business associates could take so long that a dedicated patient would run out of time before the new three-year statute of limitations for accounting records expired.

The statutory alternative would also undermine oversight. How would a patient who learned of an improper disclosure by a fourth generation business associate report the problem? How would HHS conduct oversight?

Once the rule changes to accommodate the new accounting legislation, a newspaper reporter willing to follow the accounting trail over time would eventually produce a story that exposes the new system for its inherent flaws. Even reporting the number and identity of a major health care institution's business associates might constitute an interesting news story. Suppose that a fourth generation business association of an otherwise ethical hospital did business with a subsidiary of a marketer or with a company under scrutiny for various misdeeds. A press story, even without any actual misuse of information, could be highly embarrassing.

A problem with the statutory alternative is that it removes the covered entity from the need to collect and oversee disclosures by its business associates. This is an important element of accountability within the health care system. A covered entity may never learn that its business associate is improperly disclosing patient records to marketers or others. Worse still, a covered entity could effectively hide its misdeeds behind a chain of accounting. The covered entity could direct a fourth degree business associate to make a questionable disclosure. Only an extremely determined patient willing to make a major effort over many months would ever have a chance of uncovering the disclosure.

Another consequence of a shifting of the accounting responsibility from covered entity to business associate involves authentication of patients. **The covered entity should not find authentication difficult, but a business associate may.** A business associate may have no simple way to authenticate patients, and there could be considerable expense to both patient and business associate. Further, if a covered entity has multiple business associates, each one might have to go through a separate authentication rather than a single authentication by the covered entity. The burden on patients could be overwhelming.

To minimize the problem, I suggest that we place more of the burden of producing an accounting on the covered entity with which the patient did business in the first place. That covered entity would know which of its many business associates actually received patient information during the period in question and might have additional accounting information. **A better alternative would be for the covered entity to disclose only a list of business associates to which the covered entity made disclosures about the individual in question.** That solution would cut off much, but not all, of the cumbersomeness of the process described in the statute.

8. Online Access to Accounting Records

If a covered entity provides an individual with online access to the individual's health records, it should also be required to **provide online access to accounting records**. Once the individual has been sufficiently authenticated to allow direct access to a health record, there is no reason not to allow access to accounting records in the same matter. Online access will allow individuals to monitor how their records are being used without the need for or expense of a request. The result will be better informed patients, better monitoring, and lower costs.

The direct costs will be trivial if patient access is otherwise supported. However, a patient who utilizes online access to accounting records is likely to have many questions. Most patients will be stunned about the number of uses and disclosures. The information will be educational. In order to help patients understand how records are used covered entity should be required to post information about accounting that will enable patients to figure out what the accounting records mean. A covered entity's privacy officer should take on the responsibility of educating patients. Most of the burden of providing educational materials will be a one-time expense.

9. Other Uses of Accounting Records

Many of the benefits of accounting are wasted – not because patients do not have ready access or realize that the records are available or understand how to use them – **but because covered entities do not use accounting records effectively.** Accounting records can uncover misuse of health records if covered entities are required to use them for that purpose. Everyday, there are millions of uses and disclosures of health records. How can anyone wade through accounting records for these activities? The answer is that computers can do nearly all of the work sifting through large numbers of records for discrepancies, suspicious patterns of activities, and plain improper conduct. **HHS should require every covered entity to conduct audits using computers to scan accounting records.** The results of computer scanning should be a starting point for further investigation. As we have learned from some of the stories of celebrity record snooping, a small amount of oversight and discipline can have a big payoff in greater privacy and security.

Transparency

Privacy notices are important for two primary reasons. First, notices tell patients what their rights are. Second, they tell the employees of covered entities what the rules are. Both of these functions are important.

The current HIPAA rule that asks health care providers to make good faith efforts to obtain from patients a signed acknowledgement that the patients received a privacy notice is the worst of all possible procedures. It entails lots of meaningless paperwork for a process that no one on either end of the transaction understands or benefits from.

However, that does not mean that the notices themselves do not have a value. **Notices must continue to be available in waiting rooms. Patients who ask for notices must be able to receive them. Privacy notices must be posted on the websites of covered entities.**

It is unreasonable to expect all patients to read the privacy notice. Nor should the measure of the value of privacy notices be whether patients have read or understood their rights. Patients are often sick, anxious, impaired, or have other problems that make the notice inaccessible or irrelevant to them at the moment no matter how the notice is distributed or available. However, it is crucial that the notice be available when the patient wants to read it. For some, that will be never. For others, the desire to understand or exercise privacy rights will come when they have a dispute, when they need a copy of their records, when they are told

something that sound wrong, or when they learn from a friend, relative, newspaper, or website that they have useful privacy rights. Patients will learn on their own schedules. The availability of information on the Internet makes this much easier than in the past.

Notices are important even if patients never read them. Preparing a notice forces a health care institution – or any institution – to develop a coherent and complete policy. The notice tells employees what their obligations are. It is useful and perhaps essential as a form of training and as a reference when questions arise.

How to improve notices? **Don't let lawyers write them.** Lawyers write incomprehensible verbiage. I do not know that it is possible to write a privacy notice at the eighth grade reading level, but most notices could be clearer, simpler, and more standardized.

Once you have an established set of privacy rules for health records, there should be little need to change notices except where the law changes. **Trying to affirmatively notify patients of a change in a notice is too expensive and too cumbersome.** Instead, require an institution to offer to email notice of a change to those who want to know. Few people will sign up, but that will accommodate the interest of those who care at very low cost.

There are other ways to educate patients. I was amazed at the lack of HIPAA privacy materials aimed at explaining the rights of patients. HHS provides little that is useful to the average person. Working with the World Privacy Forum, I prepared a Patient's Guide to HIPAA with 64 FAQs. http://www.worldprivacyforum.org/hipaa/index.html. When the HIPAA Guide was first posted on the web this year, there was tremendous interest. Some hospitals wanted to use it because there are so few educational materials on health privacy. HHS is not capable of producing a guide of this type because it is too bureaucratic. But it could fund outside organizations to produce educational materials without imposing editorial control. The World Privacy Forum developed and posted the Patient's Guide to HIPAA without any dedicated financial support.

You asked specifically about privacy notices after mergers and bankruptcies. These are not necessarily important events from a health privacy perspective, especially in an EHR environment. If patient records continue to exist but under the control of a new entity that is subject to the same privacy laws, regulations, and policies that applied before, no specific notice need be given to patients. If there is some major change, however, that may be a different matter. For example, if a small practice promised some patients that it would comply with specific patient requests for confidentiality, any institutional change that would undermine or eliminate the promise should lead to advance notice and should allow patients to take other steps to protect their privacy. This type of circumstance will likely arise rarely.

New or merged institutions are likely to communicate with existing patients for other purpose. If there are important changes, they can piggyback on other notices. Otherwise, changes that affect local implementation (e.g., contact information for the privacy officer, local procedures for requesting records) can be accomplished by changing the privacy notice and maintaining the old procedures for a transition period.

Personal Health Records

I offer a few summary observations about privacy and personal health records. Last year, I wrote a paper on this subject for the World Privacy Forum. *Personal Health Records: Why Many PHRs Threaten Privacy* (together with a consumer advisory) available at http://www.worldprivacyforum.org/personal_health_records.html.

1. The response to the paper was uniform. **Hardly anyone, including many sophisticated HIPAA observers, realized that most PHRs weren't covered by HIPAA**. Even seasoned health care reporters did not understand the point. Only HIPAA experts understood it.

The confusion will remain until there is a law or regulation for privacy of PHR records. This is not a unique problem. Other repositories of health records that are not subject to HIPAA can be found at gyms, life and casualty insurers, banks, credit bureaus, credit card companies. many health researchers, National Institutes of Health, cosmetic medicine services, transit companies, hunting and fishing license agencies, occupational health clinics, home testing laboratories, massage therapists, nutritional counselors, alternative medicine practitioners, marketers of non-prescription health products and foods, and some urgent care facilities.

PHRs need to be subject to privacy law because they duplicate records from the health care system. **PHR privacy rules must be much stricter than the HIPAA rules**.

2. **The biggest threat to patient privacy in the PHR space comes from commercial, advertising supported PHRs. These are essentially devices transfer health data out of legal protections and put them into the hands of marketers/profilers, where the records have the highest commercial value and where there is no regulation whatsoever.** This can only get worse because there are too many companies, and there will be a race to the bottom.

I am less worried about PHRs offered by employers or health plans because these sponsors do not want advertising that will increase their costs. My other concerns remain. If ads are allowed, then there is a distinct probability that health information will leak out without any real understanding or awareness by patients.

Commercial, advertising supported PHRs will eviscerate the health privacy interests of participants and their relatives. They also **will raise health care costs** because pharmaceutical manufacturers and others will only advertise high-cost, patent-protected products. If the advertisers do not increase revenues, they will stop advertising. If they do increase their revenues, then costs will go out without any assurance of better outcomes or offsetting cost reductions elsewhere.

3. **Consent is not the right way to control PHRs.** Websites know how to wheedle consent from consumers. We see confusing opt-outs, pre-checked boxes, unreadable terms of service, policies changeable at will, behavioral targeting, advertising that transfers PHI to marketers, search engines that record search requests and add it to consumer profiles, quizzes that exist only to collect identifiable information, and contests to win a t-shirt that result in transfer of personal

information. Consent does not work because people are lazy, busy, confused, unaware, or dazzled.

Consumers don't stand a chance without help. **The right solution is to place all PHRs under the same fiduciary obligation as physicians**. Force them to act in the best interest of patients. Physicians do not sell patient records to marketers. They didn't do so even before the HIPAA restriction because it is unethical. In ARRA, Congress strengthened the restriction on marketing under HIPAA. We need a similar rule for PHRs. PHR vendors must be forced by law to act in the best interest of their patients and not their shareholders.

Consent

Some advocate the use of patient consent as the way to control the use and disclosure of health records. That is a fantasy. **Many patients do not have the understanding, capacity, knowledge, or interest to control the disclosure of their health records by reading and signing consent forms.** Frankly, if we limited the class of patients to doctors and lawyers, many of them would also do poorly if confronted with the complex set of choices that a full consent regime requires.

Patients may have hundreds or thousands of data fields in their health records, and ten or more providers. Which providers can see which information? Which of the dozens of test results can be shared? Even orders for tests can be revealing, even if the test results are normal. How many patients can handle these decisions?

We had a consent regime before HIPAA. It didn't work. You went to see your doctor, you were handed a consent form that authorized the disclosure of all of your records to anybody. **This "informed consent" was neither informed nor consensual.** People didn't read the forms or understand them. Patients didn't have a choice. If they didn't sign the form, they couldn't see the doctor or have insurance pay the bill. It is a myth that we had an informed consent regime since third party payment became the norm for health care.

If you want proof, look to the past. In 1998, Maine passed a health privacy law that required affirmative written consent for many health disclosures. **The law was so unpopular and so impractical that the legislature suspended the law shortly after it took effect.** Many of the law's requirements for written consent were later replaced with expanded authority for nonconsensual disclosures. I wrote this short paper to provide a review of the history of the Maine law: *Consent for Disclosure of Health Records: Lessons from the Past*, available at http://www.worldprivacyforum.org/pdf/MaineHealthPrivacy1998_Gellman.pdf.

I also invite your attention to a much older, pre-HIPAA, paper I wrote that discusses the "paradox of informed consent" for the disclosure of health records. The paper remains relevant to debates over the role of consent in health care disclosures. *The Privacy of Health Information and the Challenge for Data Protection*, is available at http://bobgellman.com/rg-docs/rg-health-consent-97.pdf.

The paradox of informed consent is that giving the patient more of a say in the disclosure of health records for payment results in the patient having less actual control. Patients will be trained to sign forms without reading them. The signing of a consent form will not be an event that triggers concern or suspicion. Written by insurance companies and health care providers, consent forms allow broad disclosure without any conditions or restrictions. Health care providers – who may share their patients' concern about confidentiality – nevertheless want to be sure that they can make disclosures necessary for payment. **The effect of the standard informed consent model is to protect the interests of all parties except the patient.** In any event, there are dozens of non-consensual disclosures that are essential to the operation of the health care system. Consent is not relevant when there is no choice.

We need better controls (procedural and substantive) over nonconsensual disclosures. We also need to find a way to accommodate special situations where people have a specific need to control the flow of information or where another law (e.g., substance abuse, AIDS, genetic, mental health, pay-out-of-pocket)) applies. We simply cannot expect to use consent to control every disclosure for every patient. Finding the right balance to match privacy needs with patient capabilities and to do so within reasonable cost constraints will not be easy. In fact, this will be very difficult to do. The tradeoffs are sharp, and it is not possible to accommodate fully every relevant interest. I tell you frankly that I do not have all the answers here.

It will take a lot of hard work and wrenching choices to find the proper workable role for consent. Consent must play a role in controlling the disclosure and use of health information, but it will not be a starring role.

*****