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

September 9, 2009

Notes and Observations on Selected Parts of Title XIII, Subtitle D, Privacy
American Recovery and Reinvestment Act of 2009
Public Law No: 111-5

Selected parts of the new law are reproduced here *in italics* for convenience.
Note that parts of the new law are discussed or reproduced.
Commentary begins with ➔

You can find the complete text of Subtitle D, together with the relevant parts of the conference committee report, at http://bobgellman.com/rg-docs/Stimulus-Privacy-HIPAA.doc.

INTRODUCTION

➔ The stimulus law includes a subtitle that addresses privacy, with numerous provisions affecting the HIPAA health privacy rule. Other parts of the law, notably the other parts of the health information technology title (XIII) also address privacy in other ways. The focus here is only on the privacy subtitle.

➔This document offers personal notes and observations on selected parts of that privacy subtitle. This analysis benefited greatly from assistance provided by several people who I cannot identify, but I am grateful for their comments. Any errors are mine alone. Many of the uncertainties raised here will likely have to be resolved by the Secretary of HHS in the revised HIPAA rule.

➔ I am not much interested in the law's breach notification provisions, and I offer no analysis of the details. The enactment of distinct breach notification laws for different sectors or agencies will only lead to problems. However, I do observe that we have many state breach notification laws and at least one federal law that covers some health records (for the Department of Veterans Affairs, 38 U.S.C. § 5721 et seq.). These laws overlap with the new breach requirements, and the legislation does not address how these laws interrelate. The result could be considerable confusion, duplication of effort, and unnecessary expense. The usual HIPAA rule that the stronger law takes precedence is likely to apply here, but that may not reduce the confusion or the overlap. For example, if a state law requires reporting to a state official and HIPAA calls for reporting to HHS, both provisions will remain valid because the requirements are not contrary. The current regulation defines in detail what it means for a law to be more stringent, and this regulation (45 CFR § 160.202) may need to be amended to add a gloss of stringency in the context of breach notification laws.

• SEC. 13400. DEFINITIONS.

· *(5)* ***ELECTRONIC HEALTH RECORD****.--The term ``electronic health record'' means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.*

➔ An EHR can be created and maintained by someone who is not a covered entity. Under the definition, it appears that the EHR must be "created, gathered, managed, and consulted" by authorized health care clinicians. A comparable record maintained by an insurer or anyone else is not an EHR under this definition because an insurer is not a clinician. I don't know if this result is on purpose or by happenstance. It is also not clear what makes a clinician *authorized* or who makes the determination. It would be interesting but probably unsustainable if the patient must authorize the clinician.

➔ It may be both noteworthy and troublesome that the EHR must be "created, gathered, managed, and consulted" by clinicians. What if the clinician only does one, two, or three of these tasks? Perhaps the law should have used *or* instead of *and*, but either way is troublesome.

➔ If an EHR is also consulted by unauthorized clinicians, does that mean that the EHR falls outside the definition or does the use of an electronic record by a single authorized clinician bring the EHR under the definition? Must there be two clinicians to meet the statutory definition?

➔ Will a clinician's email system meet the definition? More broadly, will other information systems not part of a standard EHR qualify as an EHR or as a separate EHR? There is lots of sloppy language in this definition for the regulation to fix.

➔ A brief search of 42 U.S.C. did not turn up a definition for *clinician*. It must mean something other than a health care provider, however. Just what it means isn't clear. It seems an unusual term in this context.

➔ Can a record maintained by a health plan qualify as an EHR? The requirement that an EHR be created, gathered, managed, and consulted by authorized health care clinicians suggests that it could be difficult for plan records to qualify. However, an interpretation that leaves health plan records outside the scope of EHRs seems wrong. One way around this may be for HHS to use other authority to treat health plan electronic records in the same way as EHRs under the statute.

· *(11)* ***PERSONAL HEALTH RECORD****.--The term ``personal health record'' means an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.*

The definition of *PHR Identifiable health information* is:

(2) ***PHR IDENTIFIABLE HEALTH INFORMATION****.--The term ``PHR identifiable health information'' means individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information--*

(A) that is provided by or on behalf of the individual; and

(B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

The existing definition of *individually identifiable health information* is:

(6) Individually identifiable health information
The term "individually identifiable health information" means any information, including demographic information collected from an individual, that—

(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and—

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

➔ The definition of *PHR identifiable health information* importantly adds that the term includes information *provided by or on behalf of an individual*. The information provided by or on behalf of an individual does not have to be health information. Exactly when a compilation of information about an individual becomes *PHR identifiable health information* isn't clear. The definition suggests that the starting point is *individually identifiable health information*, but it is not as precise as it might be. It is possible to read the definition as including other information about an individual without any health information. That may not be the best reading, however, and the regulation can clarify.

The conference report offers some clarity too. It provides:

Another set of such modifications pertains to the definition of Personal Health Records. Specifically, the report clarifies that Personal Health Records are ''managed, shared, and controlled by or primarily for the individual.'' This technical change clarifies that PHRs include the kinds of records managed by or for individuals, but does not include the kinds of records managed by or primarily for commercial enterprises, such as life insurance companies that maintain such records for their own business purposes. By extension, a life insurance company

would not be considered a PHR vendor under this subtitle. A second clarification in the definition of PHR is the use of the term ''PHR individual identifiable health information'' (as defined in section 13407(0(2)). In the House and Senate bills, the term ''individually identifiable health information'' was used. Use of that term would have required that, to be considered a PHR, an electronic record would have to include information that was ''created or received by a health care provider, health plan, employer, or health care clearinghouse.'' However, there is increasing use of electronic records that contain personal health information that has not been created or received by a health care provider, health plan, employer, or health care clearinghouse. Use of the term ''individually identifiable health information'' would have thus improperly narrowed the scope of the term Personal Health Record under this subtitle.

Thus, the conference report included the broader term, PHR individual identifiable health information, so that the scope of the term Personal Health Record would properly include electronic records of personal health information, regardless of whether they have been ''created or received by a health care provider, health plan, employer, or health care clearinghouse.''

➔ The result suggested by the conference report seems to be the right one, but there will still be uncertainty about the scope. Consider a gym that maintains a record of a patron's activities, heart rate, and the like. That record may fall under the definition, especially if the patron has access to and contributes to the record. Much will turn on the interpretation of the requirement that a PHR be *managed, shared, and controlled by or primarily for the individual.*

➔ Consider a commercial vendor of PHR services that uses a patient record to serve ads or to otherwise market to the patient. If that vendor is financed by advertising, it may be able to argue that its records are not primarily for the patient but that the records are *managed, shared, and controlled* also for its own financial profit. That could put commercial, advertising-supported PHRs outside the definition. This is surely not what Congress intended.

➔ Others who may have *PHR identifiable health information* include some who have health information but who are not HIPAA covered entities. These could include Internet websites and search engines that focus on health matters and compile health information from browsing activities; home testing laboratories; massage therapists; nutritional counselors; alternative medicine practitioners; disease advocacy groups; marketers of non-prescription health products and foods; National Institutes of Health, and others. Much will depend on the nature of the service offered by these entities, and the degree of patient control over, involvement in, and access to records. If any of these organizations makes it easy for individuals to contribute to or access records, that may make the records PHRs in either whole or in part. If a subset of a health record is *managed, shared, and controlled by or primarily for the individual*, does that bring the whole record or the subset under the definition of PHR? However the line is

drawn, the *primarily* standard may make it easier for a record keeper to take artificial actions to bring its activities inside or outside the definition.

· *(18)* ***VENDOR OF PERSONAL HEALTH RECORDS****.--The term ``vendor of personal health records'' means an entity, other than a covered entity (as defined in paragraph (3)), that offers or maintains a personal health record.*

➔ A PHR vendor cannot be a covered entity. Whether this will turn out to be a troublesome distinction remains to be seen. There are clearly two classes of PHR providers. One consists only of covered entities, and the second includes only non-covered entities. Only those in the second class are *Vendors of PHRs* under the law.

➔ It seems possible for a covered entity to create a PHR that is not subject to HIPAA. A covered entity could create a hybrid entity that offers the PHR. Presumably, that hybrid entity would be a PHR vendor if the PHR were not maintained by the part of the hybrid entity that is a covered entity.

➔ Arguably, an individual who maintains medical records for a family member may be a PHR vendor because there is no overt requirement in the definition for any payment for the service. This was surely not the intent, and regulations may clarify the point. It may not be that easy, however, since some commercial operations that maintain records on behalf of others will also not seek payment for services. Still, exempting family members should be easy to do. Family genealogies probably should also fall outside the definitions, even though a genealogy may include considerable health information. Commercial genealogy websites could fall under the definition, however. The regulations here will require some care to capture only the right entities.

PART 1--IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

• SEC. 13401. APPLICATION OF SECURITY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES; ANNUAL GUIDANCE ON SECURITY PROVISIONS.

· *(a) Application of Security Provisions.--Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.*

➔ Three of the four cited sections are the core requirements of the security regulation for administrative, physical, and technical safeguards. The other cited section addresses policies and procedures and documentation requirements. This seems generally unremarkable, but the result is that some

provisions of the HIPAA security rule apply to business associates directly and some only by business associate agreement. It may mean that business associate agreements will need to be changed, perhaps all of them.

➔ The possibility exists that a business associate directly subject to the law will insist on higher or different security levels than the business associate's client requires. The business associate may have different requirements because the size or nature of its activities differs from those of its clients. It isn't immediately clear how the difference in application of the requirements will play out. However, when enough lawyers for different organizations become involved in figuring this out, it may get interesting and expensive.

· *(c) Annual Guidance.--For the first year beginning after the date of the enactment of this Act and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective and appropriate technical safeguards*****

➔ The requirement for annual guidance on technical safeguards could tax HHS's resources. Given the time that it may take for guidance to go through the clearance process, there is a chance that the guidance will always be out of date. Regardless, covered entities and business associates subject to the technical standards may be obliged to change their technical safeguards annually.

A later provision [§ 13402(h)(2)] – part of the security breach section – also requires annual guidance on "guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals". The importance of this guidance comes from the definition of *unsecured protected health information*. Essentially, something not secured as specified in the Secretary's current guidance is *unsecured* and the full security breach notice requirements attach. In other words, there could be annual upgrades required for encryption or other requirements. This is a mixed blessing, with the promise of better security and higher costs.

• SEC. 13404. APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES.

· *(a) Application of Contract Requirements.--In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e) of such title. The additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.*

· *(b) Application of Knowledge Elements Associated With Contracts.--Section 164.504(e)(1)(ii) of title 45, Code of Federal Regulations, shall apply to a business associate described in subsection (a), with respect to compliance with such subsection, in the same manner that such section applies to a covered entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of such title, except that in applying such section 164.504(e)(1)(ii) each reference to the business associate, with respect to a contract, shall be treated as a reference to the covered entity involved in such contract.*

➔ Subsection (b) is a convoluted provision. Existing HIPAA privacy rule section 164.504(e)(1)(ii) says roughly that a covered entity violates the privacy standard if it knew that its business associate was violating of the business associate agreement and took no action. Subsection (b) above appears to make this provision work both ways. If a business associate knows that a covered entity is violating the standards, the business associate must take action. In other words, a business associate may be independently liable for not ratting on the covered entity that hired it for the covered entity's violations of HIPAA. This may make for interesting discussions and litigation between covered entities and business associates. It may also lead to the exposure or correction of more privacy violations so it is likely to be more of a good thing from a privacy perspective, even if it makes complications for covered entities and their business associates.

• SEC. 13405. RESTRICTIONS ON CERTAIN DISCLOSURES AND SALES OF HEALTH INFORMATION; ACCOUNTING OF CERTAIN PROTECTED HEALTH INFORMATION DISCLOSURES; ACCESS TO CERTAIN INFORMATION IN ELECTRONIC FORMAT.

· *(a) Requested Restrictions on Certain Disclosures of Health Information.--In the case that an individual requests under paragraph (a)(1)(i)(A) of section 164.522 of title 45, Code of Federal Regulations, that a covered entity restrict the disclosure of the protected health information of the individual, notwithstanding paragraph (a)(1)(ii) of such section, the covered entity must comply with the requested restriction if--*

(1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and

(2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

➔ This requirement makes mandatory a patient request that a covered entity limit disclosures to a health plan if the patient pays out of pocket in full. For privacy, this is a highly desirable outcome. However, for a health care provider, it will create a requirement that will take some care to implement. Parts of a record that are medically intertwined will have to be segregable when disclose to a health plan.

➔ If health records in an electronic system are shared, a covered entity must be able to segregate specific parts of a record and to keep those parts from

being disclosed to health plans as directed by the patient. However, the same records can be shared among various health care providers because the restriction only applies to disclosures to a health plan.

➔ A secondary provider who receives restricted information from a primary provider may also be obliged to honor the patient's demand not to disclose the information to a health plan. It will have to be determined by the rule whether a patient will have to make an additional request for confidentiality to each provider that obtains the restricted record from the original provider. In cases where a patient has many providers – including some that the patient may not know about in advance (e.g., a specialist consulted by a primary physician) – the burden may be substantial. In an era of RHIOs and HIEs, this may be especially challenging.

➔ No matter what, this provision will be complicated for everyone. It also may provide a model for broader patient control over use and disclosure of the patient's record for other purposes. It may also provide a model for addressing requirements in other laws (e.g., the alcohol and drug abuse regulations in 42 CFR Part 2) that impose downstream restrictions on categories of health information.

➔ In a likely scenario, a patient pays for a genetic test out of pocket and requests confidential treatment for the test and the result. The patient, having learned that he is at risk for colon cancer, has a colonoscopy at age 30. The health plan refuses to pay on the ground that colonoscopies are not appropriate for 30 year olds. When a patient undergoes treatment based on information, a test, or a procedure that the patient has hidden from a health plan, the patient is likely to face a difficult dilemma. This may become even more complicated if the genetic test was done on a blood relation and not the patient. The relative may have placed a limit on disclosure of the information to the health plan, but the information may be freely shared within the family. The patient may be unable to satisfactorily explain an action without revealing the relative's secret.

➔ Will a health plan be told that parts of a patient's record have been withheld at the request of the patient? A request for pre-certification or for payment might be flatly denied by a health plan because any information withheld may be relevant to its decision. If plans can pressure individuals by refusing coverage, then the entire provision may be meaningless. Similar issues may arise when medical underwriting by health plans occurs.

· *(b) Disclosures Required To Be Limited to the Limited Data Set or the Minimum Necessary.—*

(1) IN GENERAL.—

(A) IN GENERAL.--Subject to subparagraph (B), a covered entity shall be treated as being in compliance with section 164.502(b)(1) of title 45, Code of Federal Regulations, with respect to the use, disclosure, or request of protected health information described in such

section, only if the covered entity limits such protected health information, to the extent practicable, to the limited data set (as defined in section 164.514(e)(2) of such title) or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.

(B) GUIDANCE.--Not later than 18 months after the date of the enactment of this section, the Secretary shall issue guidance on what constitutes ``minimum necessary'' for purposes of subpart E of part 164 of title 45, Code of Federal Regulation. In issuing such guidance the Secretary shall take into consideration the guidance under section 13424(c) and the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

(C) SUNSET.--Subparagraph (A) shall not apply on and after the effective date on which the Secretary issues the guidance under subparagraph (B).

(2) DETERMINATION OF MINIMUM NECESSARY.--For purposes of paragraph (1), in the case of the disclosure of protected health information, the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

(3) APPLICATION OF EXCEPTIONS.--The exceptions described in section 164.502(b)(2) of title 45, Code of Federal Regulations, shall apply to the requirement under paragraph (1) as of the effective date described in section 13423 in the same manner that such exceptions apply to section 164.502(b)(1) of such title before such date.

➔ Subsection (b)(1)(A) is most interesting. It applies to uses, disclosures, and requests until the Secretary issues additional guidance on *minimum necessary*. The existing rule requires covered entities to make reasonable efforts to limit uses and disclosures to the minimum necessary to accomplish the intended purpose.

➔ The new standard appears to be much more complex. A use, disclosure, or request must be limited *to the extent practicable* to a limited data set as defined in the existing rule. The minimum necessary standard only applies alternatively if the covered entity *needs* to make a use, disclosure, or request more extensive than the limited data set. If so, then a broader minimum necessary disclosure is allowable. The existing regulatory language [§§ 164.514(d)(2)(ii) & (3)(i)] about making reasonable efforts to limit disclosures is not repeated in the legislation.

➔ This new language appears to impose a greater obligation on covered entities to limit disclosures. The emphasis on the more restrictive *limited data set* is welcome from a privacy perspective because of the privacy benefits of sharing data without overt identifiers. The existing health care system does not value sharing of non-identifiable data, and the law now imposes a greater requirement to try. However, from the perspective of a covered entity, the judgments required may be considerably more complex, at least until the Secretary issues new guidance.

➔ It will help some that the exception to minimum necessary for treatment disclosures or requests is expressly continued in the legislation. The other existing exceptions are also continued.

➔ The new legislation also makes it clear that the burden of making a minimum necessary disclosure falls on the disclosing entity. Thus, the disclosing entity must determine what constitutes the minimum necessary to accomplish the intended purpose of a disclosure. The disclosing entity must decide what a researcher, public health agency, health oversight agency, and others need to accomplish their objectives. The current rule [§ 164.514(d)(3)(iii)] allows a covered entity to rely on the requester's representation that the scope of the request is the minimum necessary for the stated purpose. If that part of the rule has to be repealed, it could substantially increase the burden and liability of a covered entity making a disclosure. That has some potential to improve privacy by limiting disclosures. However, resources available for controlling disclosures are not unlimited, and putting too much burden on covered entities can create its own difficulties.

· *(c) Accounting of Certain Protected Health Information Disclosures Required if Covered Entity Uses Electronic Health Record.—*

(1) IN GENERAL.--In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information--

(A) the exception under paragraph (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information; and

(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested.

(2) REGULATIONS.--The Secretary shall promulgate regulations on what information shall be collected about each disclosure referred to in paragraph (1), not later than 6 months after the date on which the Secretary adopts standards on accounting for disclosure described in the section 3002(b)(2)(B)(iv) of the Public Health Service Act, as added by section 13101. Such regulations shall only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures.

(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.

➔ One new accounting requirement makes a positive change from a privacy perspective. Another eviscerates a significant part of the value of the accounting provisions without reducing the costs of covered entity or business associates.

➔ The first accounting change applies only to EHRs. For activities using an EHR, the existing provision that exempts disclosures for treatment, payment, and health care operations will not apply. This is a very positive step for privacy. In any electronic system, tracking all basic disclosures should be simple. The new law recognizes that. The law limits patient access to three years, a period that is much too short, especially if a covered entity retains the data anyway.

➔ The accounting provision would be much improved if it applied equally to uses as well as disclosures. An EHR system can easily track uses. Even if tracking uses is not required, a covered entity that tracks uses (and many do) should be required to disclose any accounting that it maintains and can reasonably retrieve. This is an unnecessary gap in the law.

➔ The second change 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. 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.

➔ 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. One limiting factor will be the unwillingness of some covered entities to reveal the number or identity of their business associates. A hospital may be unwilling to tell patients that it employs the Type-By-Night transcription service in a third world country.

➔ 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 may have its own lawyers, accountants, computer providers, and others that would also be subject to accounting.

➔ A simple request by a patient seeking to find the source of a specific improper disclosure could require many hours of time and hundreds of dollars for postage and printing. It could also take considerable time 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. The costs would increase further if a patient reported accounting noncompliance to the parent covered entity or to various intermediate business associates. 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. Suppose that a fourth generation business association of an otherwise ethical hospital did business with a subsidiary of a company under scrutiny for various misdeeds?

➔ A single determined patient with potentially hundreds of places to search for an accounting after a single encounter with a hospital could impose a burden on the system and, ultimately, on administrative enforcement. All of these possibilities would be significantly minimized if the burden of producing an accounting fell on the covered entity with which the patient did business in the first place. That covered entity would know which of its dozens of business associates received patient information and might have additional accounting information for the requesting patient. An alternative would be for the covered entity to disclose only a list of business associates to which the covered entity made disclosures. However, because there are many types of disclosures for which a covered entity need not maintain an accounting, this partial solution may be out of reach.

➔ By removing the covered entity from the need to collect and oversee disclosures by its business associates, an important element of accountability within the health care system may vanish. A covered entity may never learn that its business associate is improperly disclosing patient records to marketers. Worse still, a covered entity could effectively hide 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 handle the authentication problem, 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 expensing of authentication could require revision of business associate contracts.

· *(d) Prohibition on Sale of Electronic Health Records or Protected Health Information.*

· *(1) IN GENERAL.--Except as provided in paragraph (2), a covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any protected health information of an individual unless the covered entity obtained from the individual, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization that includes, in accordance with such section, a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual.*

➔ This provision says that a covered entity or business associate cannot *directly or indirectly receive remuneration in exchange for any protected health information*. What does that mean? It would appear to prohibit sale of PHI. However, in the marketing business, consumer information is not normally sold. A buyer of a marketing list acquires the right to make a one-time use of the list. In the traditional model, the list is typically given to a trusted third party (letter shop) who prints and mails using the list. The list buyer never has possession of the list.

➔ Does the word *exchange* mean that the prohibition is limited to an activity that involves the transfer of PHI? If a drug company pays a hospital to send an advertisement to patients with a particular disease, has there been an *exchange* of PHI? One may argue this point on either side. The word *indirectly* clearly helps on the privacy side of the argument. However, the law might have been clearer if it said that a covered entity may not directly or indirectly receive remuneration by selling, renting, transferring, making use of, exploiting, or allowing others to exploit PHI. The regulations will have to clarify.

➔ An interesting provision here says that a patient authorization for a remunerated activity must include "a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual." Whether there will be many *remuneration authorizations* by patients is not clear. One reader suggested that any patient authorized disclosure could fall under this requirement if the covered entity merely charges for copying of a record. A copying charge may or may not qualify, and HHS could narrow the issue in its regulation. Still, there may be no grounds for excluding copying charges altogether. Copying for treatment may be more favored, but copying for marketing may be another thing entirely.

➔ What happens when the patient checks the box and prohibits further remunerated exchanges? If the recipient is a covered entity, compliance with the patient's restriction will presumably be a requirement of the rule. There still may be problems. Imagine that a covered entity receives records subject to a

remuneration exchange prohibition. The same covered entity may already have or may produce in the future records not subject to the restriction. It may also have independently the same data fields that are subject to restriction in the newly received records. How will the covered entity be able to proceed? The easiest, safest, and most privacy protective answer is that a covered entity should not engage in any remunerated activity. Those who profit from prescription reminders may not like that answer, but it is likely to be the recommendation of a conservative HIPAA lawyer.

➔ If the recipient is not a covered entity, how can HHS or the patient enforce the restriction on further exchanges? This question is left as an exercise for the lawyers, with the preliminary suggestion that there is no apparent enforcement mechanism at the federal level. State law may help patients here.

➔ What happens if the standard authorization form required by a covered entity includes the check box prohibiting further remunerated exchanges, and a patient checks the box for a disclosure to which it does not apply under the statute? Will the restriction apply anyway to the recipient? This is another interesting question with good arguments on both sides. What probably won't be arguable is the difficulty of explaining any of this to patients.

➔ What does *remuneration* mean? This is an interesting question raised by a reader. Another interesting issue is what does *payment* mean in § 13406(a) relating to marketing, and how do *payment* and *remuneration* relate. It's hard to believe that the use of these two different terms that probably should have the same meaning was anything other than a remnant of midnight drafting. One concern is that each term may have a definition in some health care law or rule, and HHS may feel some obligation to honor the existing definitions. There is, for example, this definition of *remuneration* in the Stark regs at 42 C.F.R. § 411.351:

Remuneration means any payment or other benefit made directly or indirectly, overtly or covertly, in cash or in kind, except that the following are not considered remuneration for purposes of this section:

(1) The forgiveness of amounts owed for inaccurate tests or procedures, mistakenly performed tests or procedures, or the correction of minor billing errors.

(2) The furnishing of items, devices, or supplies (not including surgical items, devices, or supplies) that are used solely to collect, transport, process, or store specimens for the entity furnishing the items, devices, or supplies or are used solely to order or communicate the results of tests or procedures for the entity.

(3) A payment made by an insurer or a self-insured plan (or a subcontractor of the insurer or self-insured plan) to a physician to satisfy a claim, submitted on a fee-for-service basis, for the furnishing of health services by that physician to an individual who is covered by a policy with the insurer or by the self-insured plan, if--

(i) The health services are not furnished, and the payment is not made, under a contract or other arrangement between the insurer or the self-insured plan (or a subcontractor of the insurer or self-insured plan) and the physician;

(ii) The payment is made to the physician on behalf of the covered individual and would otherwise be made directly to the individual; and

(iii) The amount of the payment is set in advance, does not exceed fair market value, and is not determined in a manner that takes into account directly or indirectly the volume or value of any referrals.

➔ Many routine and legitimate activities in the health care system involve remuneration or payment. If the provisions are read broadly, then the effect could be broad and catastrophic. I assume that HHS will find a way to limit the restrictions to marketing and other similar activities that inappropriately affect patient privacy. The Secretary's ability to create exceptions (see § 13405(d)(2)(G) below) will help here. I do not anticipate that the Secretary will exceed the intent of the provision notwithstanding its potentially broad language.

· *(2) EXCEPTIONS.--Paragraph (1) shall not apply in the following cases:*

(A) The purpose of the exchange is for public health activities (as described in section 164.512(b) of title 45, Code of Federal Regulations).

(B) The purpose of the exchange is for research (as described in sections 164.501 and 164.512(i) of title 45, Code of Federal Regulations) and the price charged reflects the costs of preparation and transmittal of the data for such purpose.

➔ What is interesting here is that disclosures for research may be compensated, but the price must be limited to the cost of preparation and transmittal. The actual phrase in the statute is that the price must *reflect* costs. It isn't clear whether *reflect* means *limit* or whether a price based on a multiple of cost would be allowed. The regulations will have to clarify. A later provision calls on the Secretary to evaluate the impact of the cost restriction, and the Secretary may further restrict the allowable charge. In any event, the researcher who contests the costs charged by a covered entity is likely to end up with nothing, since there is no requirement that a covered entity disclose to a researcher. One unnamed observer asks interestingly whether the limit here will prevent a drug manufacturer from giving kickbacks to a doctor for prescribing the manufacturer's drugs under the guise of data preparation costs.

· *(C) The purpose of the exchange is for the treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent protected health information from inappropriate access, use, or disclosure.*

➔ The exception for treatment is both understandable and a potential loophole. Treatment means *the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third*

party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

➔ Most treatment disclosures require that there be a health care provider on the receiving end. If that provider is a covered entity subject to the rule, then the loophole here is smaller. But the definition allows coordination or management of health care by a provider with a third party. That could be a major loophole if a provider "coordinates care" with a third party marketing firm that pays the provider so that it can send treatment-related advertising (e.g., a pharmaceutical switch letter) to patients. If there is a loophole here in fact, the regulation can and should close it.

➔ The existing definition of marketing already excludes activities for treatment. That may make the new language less troublesome. However, the new language about *exchange of PHI* complicates matters somewhat, but not beyond the ability of the Secretary to clarify.

· *(D) The purpose of the exchange is the health care operation specifically described in subparagraph (iv) of paragraph (6) of the definition of healthcare operations in section 164.501 of title 45, Code of Federal Regulations.*

· *(E) The purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement.*

➔ Subparagraph (E) is somewhat obscure. It allows a covered entity to give remuneration to a business associate for an exchange of PHI at the request of a covered entity. Just what activities this covers is not clear. One possibility is some quality improvement (QI) activities. A provider contributes PHI to a business associate conducting QI for several different providers. The business associate analyzes each provider using the jointly supplied data, and it gives an analysis back to each provider. The PHI from the covered entity and the analysis from the business associate are the remuneration. That type of transaction, seemingly allowed by subparagraph (E), may not be troublesome. Another type of activity allowed by (E) may be exchanges between covered entities and RHIOs. Those exchanges may also be less troublesome. However, the provision may allow other forms of data exchange that raise more privacy concerns.

·*(F) The purpose of the exchange is to provide an individual with a copy of the individual's protected health information pursuant to section 164.524 of title 45, Code of Federal Regulations.*

(G) The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate as the exceptions provided in subparagraphs (A) through (F).

➔ The Secretary can create additional exceptions. That may be a useful safety valve as long as the authority is used appropriately.

· *(e) Access to Certain Information in Electronic Format.--In applying section 164.524 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual--*

(1) the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific; and

(2) notwithstanding paragraph (c)(4) of such section, any fee that the covered entity may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than the entity's labor costs in responding to the request for the copy (or summary or explanation).

➔ Generally, this is a helpful provision for supporting patient access to records. The ability to direct a copy directly to a person designated by the individual will clear up some confusion that has developed about getting a copy to the individual's lawyer. On the other hand, notwithstanding the *clear, conspicuous, and specific* requirement for an individual's direction to the covered entity to transmit a copy directly to a third person, this new provision may be subject to abuse. Patients may unwittingly sign broad disclosure authorizations. For example, a direct marketer can include an authorization in a contest form. A marketer could also pay a patient for consent if the costs of the records are small enough. Records so obtained can be exploited for marketing purposes for the patient's lifetime and for the lifetime of the patient's relatives and descendants. A covered entity may have no basis for refusing to send a record to a marketer. A covered entity should have, at least in some circumstances, the ability to question a patient's intent when directing copies to some third persons.

➔ The limit on cost of electronic copies to labor costs may affect existing commercial services that support record sharing for hospitals. If that lowers the cost of patient access, the result will be good for privacy.

• SEC. 13406. CONDITIONS ON CERTAIN CONTACTS AS PART OF HEALTH CARE OPERATIONS.

· *(a) Marketing.--*

(1) IN GENERAL.--A communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations, unless the communication is made as described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of such title.

➔ Under the existing rule, it is not always clear whether an activity is treatment, a health care operation, or marketing. The definitional borders are not

sharp, and it is not clear that they can be refined with precision. The new language helps by saying that a covered entity cannot encourage use of a product or service by calling it a health care operation. This will force recommendations to be either treatment or allowable marketing activities. The clarification helps considerably from a privacy perspective.

➔ The word *encourages* may turn out to be a weasel word. Consider a drug advertisement that tells patients about an *ailment* and directs them to ask their doctor for treatment. No actual product or service is mentioned in the ad. None need be specified because only one manufacturer makes a drug for that ailment.

· *(2) PAYMENT FOR CERTAIN COMMUNICATIONS.--A communication by a covered entity or business associate that is described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of title 45, Code of Federal Regulations, shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations if the covered entity receives or has received direct or indirect payment in exchange for making such communication, except where--*

(A) (i) such communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication; and

(ii) any payment received by such covered entity in exchange for making a communication described in clause (i) is reasonable in amount;

➔ This provision allows limited marketing activities. Essentially, it allows a pharmacy to send a prescription reminder to patients paid for by a drug manufacturer. Because the communications are limited to a drug currently being prescribed, the provision prohibits the more objectionable *switch* letter, seeking to induce a patient to obtain a prescription for a different but perhaps equivalent drug. It is unclear if the language effectively prohibiting *switch* letters would apply to a letter that urged a patient to switch to generic drugs. In the interest of reducing health care costs, the Secretary could decide that a generic drug is not covered by the *switch* prohibition. (Where funding for a generic drug *switch* letter would come from is not clear.)

➔ The limit on payment to a *reasonable amount* is interesting. An earlier version of this language was limited to cost. Once the government allows marketing use of patient information by covered entities, it isn't clear why there is a need to regulate the cost. The drug manufacturers and the pharmacies can negotiate their own prices, without the need for a cap on the price that can only benefit the drug manufacturers.

➔ One consequence of the provision clearly allowing refill reminders is that pharmacies may not be the only source of information. The same information may be available from providers, plans, and PBMs. There could be a brisk competition in the market for the sale of patient information, and that could keep the price down for the benefit of drug manufacturers. Every covered entity with

access to the information (and that information could be widely available in an EHR system) may seek to be the recipient of the "reminder" payments.

➔ There may be some confusion in the language here. In the beginning, the text says *covered entity or business associate*. In other places, however, it just says *covered entity*. This may need technical correction. The same issue may arise in the next two subparagraphs.

➔ The provision allowing refill reminders would be <u>much improved</u> if it included a requirement that all communications be *non-discriminatory*. Any reminder program should cover all patients receiving a drug, regardless of age, sex, race, health status, type of health or drug insurance, or price paid for a drug. There have been some suggestions that letters are sent selectively to patients. Patients with plans that pay higher prices may be more likely to receive letters than those with plans that have negotiated lower prices.

➔ A reader asked if the marketing exceptions for face-to-face communications and promotional gifts of nominal value (45 CFR § 508(a)(3)) will survive the new legislative language. These activities involve no exchange of information so it would appear that HHS could keep the exceptions with respect to activities for which a covered entity receives no remuneration. But if a promotional gift qualifies as a *communication*, no remuneration is allowable. If a drug manufacturer gives pens to a covered entity for distribution to patients, it could arguably qualify as indirect remuneration to the covered entity.

· *(B) each of the following conditions apply--*

(i) the communication is made by the covered entity; and

(ii) the covered entity making such communication obtains from the recipient of the communication, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization (as described in paragraph (b) of such section) with respect to such communication; or

· *(C) each of the following conditions apply--*

(i) the communication is made by a business associate on behalf of the covered entity; and

(ii) the communication is consistent with the written contract (or other written arrangement described in section 164.502(e)(2) of such title) between such business associate and covered entity.

➔ In order for a refill reminder program to be lawful, it must meet one of two alternate sets of conditions. The first requires the communication to be made by the covered entity pursuant to a patient authorization. This is not new. Anything is possible under current law with an authorization. The second set of conditions calls for the communication to be made by a business associate for a covered entity <u>and</u> for the communication to be consistent with the contract between the business associate and covered entity. This is mostly unremarkable.

It stops business associates from sending refill reminders without authorization from the covered entity.

➔ An alert reader pointed out an ambiguity here. Paragraph (2) has three important subparagraphs, A, B, and C. There is no *and* after A. There is an *or* after B. So one reading is A *or* B *or* C. Another reading is A *and* (B *or* C). I adopted the second reading. It is the only one fully consistent with the legislative history. It says: "The conference report makes an exception and allows providers to be paid reasonable fees as determined by the Secretary to make a communication to their patients about a drug or biologic that the patient is currently prescribed."

➔ If the provision is read as A *or* B *or* C, then the important limitation in A can be ignored. That would ignore the conference report language. B does nothing but require an authorization, which is irrelevant or at least not new. If C stands alone, then it would not be necessary to limit allowable communications to reminders. Anything would be allowed, and that is not what Congress intended. HHS can clarify this issue in the regulations.

➔ The entire marketing subsection is badly written and smells of a last minute addition of C. The same alert reader also wondered why the non-consensual reminders allowed by C are only permitted if made by a business associate and not if made by a covered entity. That is a good question, and it is probably another place where the legislation fails to treat both covered entities and business associates properly. It is not as clear that HHS can write regulations that allow covered entities to send reminders without going through business associates because the language is so clear. It would probably be worth a try, however. Why should business associates alone have all the fun? It makes little sense that covered entities are prohibited from doing something that their business associates can do.

➔ What happens if a covered entity maintains a website and shows advertising on the website? If advertising encourages the purchase or use of a good or service (and most advertising does), then there is a strong argument that this section prohibits the advertising. It doesn't matter if the ad promotes a not-health related product. None of the exceptions is likely to apply. One can try to distinguish between targeted and untargeted ads, but it may not help because the language here is pretty broad.

➔ A comparison with the existing rule is interesting and instructive. The current rule [§ 164.508(a)(3)] bans use or disclosure of PHI for marketing, so a website ad that does not use or disclose PHI (e.g., a non-targeted ad) is possibly permissible. The difference is that the new language in (a)(2) is not tied to use or disclosure of PHI so its effect may be much broader. Any existing covered entity doing any kind of behavioral advertising, even if based only on cookies, may arguably be violating the existing rule. If a covered entity sets a cookie, the

cookie may be PHI. So may an IP address. When patients sign in to use the website, these conclusions are easier. Everything about an existing, identifiable patient is PHI. If the covered entity's website only has the cookie or IP identifier and no other information about the user, it is a harder question whether there is information "that identifies the individual" or whether the information relates to health within the meaning of the existing rule definition. Whether an IP address is identifiable is a much disputed question generally.

· *(b) Opportunity to Opt Out of Fundraising.--The Secretary shall by rule provide that any written fundraising communication that is a healthcare operation as defined under section 164.501 of title 45, Code of Federal Regulations, shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication. When an individual elects not to receive any further such communication, such election shall be treated as a revocation of authorization under section 164.508 of title 45, Code of Federal Regulations.*

➔ There is very little new here other than the words *clear and conspicuous*. An earlier draft of the legislation prohibited fundraising altogether. The existing rule gives patients the right to opt-out. Nothing in the law or the existing rule says that patients may opt-out by phone, email, or orally. It would be useful if all of the above had to be recognized. The effect of the new language treating an opt-out as a revocation is to prevent a covered entity from denying services to a patient who has opted-out of fundraising. That is useful only to the extent that a covered entity says *accept fundraising requests or die*.

• SEC. 13407. TEMPORARY BREACH NOTIFICATION REQUIREMENT FOR VENDORS OF PERSONAL HEALTH RECORDS AND OTHER NON-HIPAA COVERED ENTITIES.

➔ The law imposes breach notification requirements on vendors of PHRs. This is interesting mostly because it marks the first federal regulation of PHR vendors. It gives regulatory authority to the FTC and not HHS.

• SEC. 13408. BUSINESS ASSOCIATE CONTRACTS REQUIRED FOR CERTAIN ENTITIES.

Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations and a written contract (or other arrangement) described in section 164.308(b) of such title, with such entity and shall be treated as a business associate of the covered entity for purposes of the provisions of this subtitle and subparts C and E of part 164 of

title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this title.

➔ This provision clarifies that regional health information exchanges, regional health information organizations, and others must have business associate contracts. There has been some uncertainty about the status of these organizations under HIPAA, and this change is positive for privacy because it closes regulatory loopholes.

➔ This language is especially interesting: *each vendor that contracts with a covered entity to allow that covered entity to offer a PHR to patients as part of its EHR* must sign a business associate agreement. That may break some new ground. A PHR vendor, even one with some type of arrangement with a covered entity, may not be subject to HIPAA under current rules. The PHR vendor may obtain records from a covered entity with patient consent. The PHR vendor provides services to the patient and not to the covered entity. This is not the only model, but it seems to be a common one.

➔ Under the new language, a PHR vendor that strikes a deal with a covered entity will be a business associate. There may be loopholes here, however. Will the offering be *part of the covered entity's EHR*? Overall, however, the effect of the new language may be to force PHR vendors to operate under HIPAA if they want covered entities to funnel patients to them. That seems appropriate. A PHR that is not subject to HIPAA can be used in ways that undermine patient privacy. See generally my report for the World Privacy Forum, ***Personal Health Records: Why Many PHRs Threaten Privacy*** **at** http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf**. The congressional purpose may be to force or pressure all PHRs to operate under HIPAA, and that would be a better result than wholly unregulated PHRs.**

➔ However, an advertising supported PHR vendor may find it difficult to survive under HIPAA disclosure limits. A PHR vendor will likely be unable to target advertising or mix its PHR records (and PHR usage records) with other records (unrelated to health) that the PHR vendor may maintain otherwise. Advertising supported PHRs may need to be wholly independent of covered entities to exploit patient records profitably, but a connection to a covered entity may be necessary to attract a critical mass of patients.

➔ On related front, the definition of *health care operation* or *treatment* may need to be changed to specify that providing a PHR to a patient is covered. It may not be clearly covered under the existing rule.

• SEC. 13409. CLARIFICATION OF APPLICATION OF WRONGFUL DISCLOSURES CRIMINAL PENALTIES.

➔ This closes the criminal penalty loophole created by the DOJ Office of Legal Counsel Opinion. See http://www.usdoj.gov/olc/hipaa_final.htm. This is a welcome change although not an essential one because clever DOJ prosecutors found other ways to prosecute offenders despite the OLC opinion.

• **SEC. 13410. IMPROVED ENFORCEMENT.**

➔ Existing law [42 U.S.C.§ 1320d-5(b)(1))] prevents the Secretary from imposing a penalty on anyone for an act that is subject to a criminal offense under 42 U.S.C. § 1320d-6 (Wrongful Disclosures). That tied the Secretary's hands in cases where the Justice Department declined to prosecute. Section 134010(a)(1)(A) changes that policy. The new language only limits the Secretary's authority in cases where someone has actually been convicted. This is a useful change that will enhance administrative enforcement.

➔ Improved enforcement changes are welcome from a privacy perspective. It should be taken by HHS as a sign that Congress is unhappy with the current state of virtual non-enforcement.

➔ A new provision that shares civil penalties with harmed individuals is not likely to be effective because another new provision allows OCR to keep penalties. OCR will have a conflict of interest in administering the sharing of penalties with individuals. The more it has to give out to individuals, the less it gets to keep. This will prove an unsustainable conflict in the long run. Aggrieved individuals will fight amongst themselves for a bigger share of the penalties, and much of the money will consumed in administrative challenges. It may be worse if a court decides that receiving a share of the civil penalty prevents recovery in a state court civil suit over the same conduct.

➔ Another new enforcement provision allows State Attorneys General to enforce the HIPAA rules. This change is welcome from a privacy perspective, but the health care industry will surely hate it. The reality is that the more significant consequences of a violation of HIPAA will come from adverse publicity rather than from legal enforcement efforts. Formal enforcement will help to feed that publicity, but it is not likely to add significantly to the costs. Lawyers will, however, continue to scare their health care clients about enforcement possibilities.

***

Document History

Version 1.81: More typos fixed.
Version 1.8: Added some relevant text from § 13405 that had not been included. Minor edits in the same vicinity.

Version 1.7: Revision of the discussion about the definition of EHRs in § 13400 to consider whether a health plan can have an EHR; new point about the effect of § 13406(a) on website advertising. These observations grew out of a CDT discussion of the new law.

Version 1.6: Some mild language changes and minor clarifications here and there; discussion of the clarifying effect of 13405(e) (Access to Certain Information in Electronic Format) on getting a copy of a record to the patient's lawyer; a new discussion in § 13405(d) about the meaning of *remuneration* and its relationship to *payment*.

Version 1.5: Slight revision of the discussion of security breach law preemption in the introduction; mild revision of discussion of definition of EHR in § 13400; addition of authentication discussion in the business associate accounting part of § 13405(c)(1); a new discussion of the secondary remuneration exchange prohibition in § 13405(d)(1); and a new discussion of the effect of § 13406(a)(2) on the marketing exceptions in § 16508(a)(3) of the current rule. Some of the new points were inspired by a discussion of the new HIPAA provision sponsored by the Center for Democracy and Technology. Other changes are the result of reader comments and questions. I am grateful for everyone's insights, but I remain responsible for the commentary.

Version 1.4: Added to the discussion of the marketing in § 13406.

Version 1.3: Added analysis of the PHR vendor language in § 13408

Version 1.21: Fixed a typo.

Version 1.2: Revised based on comments from various individuals. First Public Version.

Version 1.1: Circulated on a limited basis for comment.

This document is maintained at http://bobgellman.com/rg-docs/Stimulus-Privacy-HIPAA-Analysis.pdf.