September 13, 2010

The Honorable Kathleen Sebelius
Secretary
U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, S.W.
Washington, DC 20201

Attention: HIPAA Modifications, RIN0991-AB57

Re: Confidentiality Coalition Comments to Notice of Proposed Rulemaking on Modifications to the HIPAA Privacy, Security and Enforcement Rules

Dear Secretary Sebelius:

The Confidentiality Coalition respectfully submits these comments in response to the Department of Health and Human Services' Notice of Proposed Rulemaking on Modifications to the HIPAA Privacy, Security and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act (the "HIPAA Proposed Rule"), published in the Federal Register on July 14, 2010.

In this response, we (i) provide background on the Confidentiality Coalition; (ii) offer comments to improve the provisions of the HIPAA Proposed Rule; and (iii) respond to various issues raised by the HIPAA Proposed Rule.

Background

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health produce distributors, pharmacy benefit

managers, pharmacies, health information and research organizations, patient groups, and others[1] founded to advance effective patient confidentiality protections.

The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enable the essential flow of information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life enhancing medical interventions. The Confidentiality Coalition is committed to ensuring that consumers and thought leaders are aware of the privacy protections that are currently in place. And, as healthcare providers make the transition to a nationwide, interoperable system of electronic health information, the Confidentiality Coalition members believe it is essential to replace the current mosaic of sometimes conflicting state privacy laws, rules, and guidelines with a strong, comprehensive national confidentiality standard.

Discussion

The Confidentiality Coalition generally applauds the Department's efforts to fulfill its obligations under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") and to reasonably implement changes to the HIPAA Privacy, Security and Enforcement Rules that address the relevant statutory mandates. On the whole, the Confidentiality Coalition believes that the Department has done an effective job of addressing the relevant statutory provisions in a way that appropriately protects individual privacy without raising undue concerns among patients or unduly increasing compliance obligations for the healthcare industry and its business partners. In this letter, the Confidentiality Coalition offers comments and constructive suggestions in response to several particular provisions of the HIPAA Proposed Rule.

1. HIPAA Subcontractors

We understand and appreciate the Department's interest in ensuring that the privacy and security of protected health information is appropriately secured when PHI is provided to subcontractors. However, we have significant concerns about the effect of the proposed provisions related to subcontractors and the approach taken by the Department in this regard.

First, as a general matter, we do not read the legislative provisions of HITECH as extending full HIPAA compliance obligations to subcontractors. It is our view that the legislative language applies only to business associates who contract directly with HIPAA covered entities. Therefore, there is both a question as to the Department's authority to create new legal obligations for HIPAA subcontractors as well as an opportunity to protect information held by these subcontractors without going as far as the new obligations for business associates.

[1] A list of the Confidentiality Coalition members is attached to this letter.

Second, on a more substantive level, we do not believe that it is necessary to extend full HIPAA compliance obligations to these HIPAA subcontractors, many of whom may be quite distant from the core operations of the healthcare industry. Under the current HIPAA rules, all HIPAA subcontractors should have in place with their business partners (both upstream and downstream) a HIPAA agreement that incorporates the required provisions of a business associate agreement. It is and has been a requirement of all business associate contracts that the business associate impose on its subcontractors the obligation to follow the particular contractual terms dictated by the HIPAA Privacy and Security Rules. Therefore, we do not agree with the Department's assertion that privacy and security protections "lapse" when PHI is provided to subcontractors.

With that said, we do not see a significant impact from the Department's extension of *Privacy Rule* legal obligations to these subcontractors. These obligations should not affect ongoing operations, since these subcontractors already must meet the contractual obligations imposed by a business associate contract. We do not object to the effort to impose on these subcontractors a legal obligation to follow the terms of a business associate contract. Given the focus of this provision on the contractual terms required by the Privacy Rule, this step will not require operational changes for subcontractors, but will merely change the legal effect of a failure to meet these terms.

Where we disagree with the Department's approach involves the obligations under the HIPAA Security Rule. We understand that HITECH now imposes on business associates the legal obligation to meet all of the obligations of the HIPAA Security Rule. While we recognize that Congress has mandated this step, this is a significant challenge for many business associates, particularly those for whom the healthcare industry is only one component of a broader business operation. It is relatively easy to set up Privacy Rule procedures that address specific work projects that involve PHI, without the need to apply these procedures to other aspects of a company's business that are outside the scope of HIPAA. This is much more difficult under the Security Rule, because companies typically do not utilize separate computer systems for their HIPAA business. This problem exists currently. This new obligation would require subcontractors to engage in significant efforts to review overall security practices that likely will apply across a company's business (given the nature of most electronic systems), even if HIPAA-covered activity is only a small portion of the work of a subcontractor. We also are aware of a substantial number of situations where subcontractors do not even know if they will be receiving protected health information in the course of an engagement, yet this obligation would require a substantial remediation effort in advance of performing any work (again, unlike the Privacy Rule, where procedures can be implemented at the time of receiving PHI, without the need for a significant investment in advance).

Therefore, we believe that applying this principle to all subcontractors will impose significant hardships on many subcontractors, and may even force some subcontractors from the healthcare marketplace, without significant additional privacy and security protections for PHI. If potential contractors are eliminated from the market, costs will increase without the benefit of enhanced

security. Instead, we propose an alternative modeled on the Privacy Rule approach – imposing on subcontractors a legal obligation to follow the security-related terms of a business associate contract. This would include (consistent with 45 C.F.R. 164.314(a)(2)(i)(A)) the obligation to "[i]mplement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity [or business associate.]" While we support a change that would impose a legal obligation (and not just a contractual obligation) on a subcontractor to follow this requirement, this approach would not require subcontractors to engage in the full set of technical, physical, and administrative safeguards and policies and procedures that are required by the HIPAA Security Rule for covered entities and business associates that contract with them directly. We believe that this approach would reasonably protect PHI while not imposing undue burdens on subcontractors. Moreover, this step would moderate additional complications to the business associate contracting process, as subcontractors and their business partners would not need to engage in new discussions about the details of HIPAA Security Rule compliance and the question (which we are seeing raised on an increasing basis) as to whether a particular vendor meets the definition of a subcontractor for HIPAA purposes.

If the Department does use its regulatory authority to require subcontractors to meet all of the legal obligations of the Security Rule, we urge the department to provide additional time for subcontractors to implement their full compliance steps or for business associates to switch subcontractors if a subcontractor will no longer perform services involving protected health information.

2. Revised Business Associate Contracts.

We support the idea of giving covered entities additional time periods to adopt revised business associate agreements. At the same time, we have significant concerns about certain statements in the HIPAA Proposed Rule that seem to require specific new wording in business associate agreements, regardless of the relevant timeframe. While the HIPAA Proposed Rule provides this additional time as a formal compliance matter, covered entities across the country have been engaged in significant efforts since the HITECH law was passed to develop and implement new business associate agreements for their relationships. Until the HIPAA Proposed Rule was published, most covered entities believed that they were under a legal obligations to revise these agreements by the effective date of the new HITECH provisions in February 2010 (or had already moved to revise their agreements consistent with the effective date of the breach notification rule). It is unfair and unnecessary to require contracts to be revised again, simply to add specific new words that were incorporated solely by the HIPAA Proposed Rule.

The particular language that raises our concern is the proposed addition to 45 C.F.R. 504 (e) (2) to add new subparagraph (H). This paragraph provides that "To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation." Our concern

with this language is not with the concept – we understand and agree that a business associate who has been retained to perform a service with specific HIPAA requirements needs to meet those requirements. Our concern, however, is with the obligation to add this language to existing business associate contracts. This is new language, and not language that could have been reasonably predicted from HITECH itself. This is essentially a requirement to add to a contract the obligation of a business associate to do what the contract says the business associate must do. If this language is maintained in the final Rule, it will require an additional modification of thousands upon thousands of business associate contracts that already have been amended since the passage of HITECH, solely to add this new paragraph. We do not see the reasonable benefit of requiring this step. There are other ways for the Department to enforce a failure to perform a HIPAA-required service than to mandate this new language in business associate contracts. We strongly recommend that the requirement to include this new language be eliminated from any final rule.

3. Covered Entity Responsibility for Business Associate Activities.

We also have a significant concern about an apparent increase in the potential responsibility of covered entities for the activities of their business associates. As we read the HIPAA Proposed Rule, the Department is proposing that covered entities now may face liability for the actions of their business associates when the business associate is acting as an "agent" of the covered entity under the federal common law of agency. We have two concerns about this proposal. First, we do not feel that the concept of the federal common law of agency is well understood or is otherwise useful in this area. If the Department continues to use this concept (which also is applicable under the interim final rule on breach notification), we believe it important for the Department to prepare a summary or other guidance on this "federal common law of agency," so that each covered entity and business associate has a mutual understanding and is not forced to develop its own view of this concept.

On a broader basis, however, we do not understand the rationale for expanding a covered entity's potential liability for the actions of its business associates, particularly now that these business associates have their own specific legal obligations under these provisions. (We have similar concerns about the responsibility of a business associate for the actions of its subcontractors.) Under the original HIPAA rules, a covered entity appeared to only have the obligation to take action against a business associate in connection with the contract, where the covered entity knew of a pattern or practice of violating the HIPAA rules. We do not support any expansion of covered entity liability for the actions of business associates.

4. Marketing

A. Treatment Distinction

We understand and support the Department's efforts to implement the HITECH marketing provisions. We appreciate the distinction that is drawn in the HIPAA Proposed Rule between

"health care operations" marketing (which typically is "population based") and treatment-related communications (typically, "patient based"). The HITECH Act placed restrictions on paid communications only to the extent those communications constituted healthcare operations, and not treatment. We support this distinction in the HIPAA Proposed Rule and believe it is consistent with Congressional intent. In fact, we believe the language in Section 13406(a)(2) is clear on this point. Specifically, Congress states in section 13406(a)(2) that the covered entity's receipt of payment in exchange for making certain communications that would otherwise constitute healthcare operations transforms those communications into marketing. Since treatment communications would not be healthcare operations' communications in the first instance, it is clear that Congress did not intend to encompass these communications in this provision. To avoid any doubt about this, Congress explicitly stated in section 13406(a)(4) that payments referred to in paragraph (2) of section 13406(a) (i.e. for certain health-related communications) *do not* include payments for treatment.

Therefore, we encourage the Department to retain the proposed distinction between treatment-related communications and other forms of marketing communications that may require authorizations. Even with this distinction, we are concerned, from a public policy perspective, that it is not wise to even permit an opt out process for treatment communications, whatever form they may take (obviously, these policy arguments are even stronger if an authorization approach were taken). By their nature and purpose, treatment communications are communications that address a particular patient's medical condition, even if they recommend a product or service in order to do so. It is hard to imagine how a healthcare provider could effectively treat a patient without communicating with that patient (or his or her personal representative) about that treatment. This is the case irrespective of whether the treatment communication has a "payment" component or not. In fact, because many of these treatment communications may involve specific patient risks, and since patients are often unaware of the dangers, they may choose to opt out of receiving them, particularly on a going forward basis, without a full understanding of the future implications.

Since treatment communications are integral to the treatment function, we do not believe it is a viable or realistic option to not send patients communications about their treatment, and therefore, not a choice that patients should be asked to make. In fact, if a patient were to opt-out of future communications, we are concerned about how healthcare providers will effectively provide treatment, if their appropriate medical suggestions are precluded by an opt-out that previously was made. It is precisely for this reason that Congress carved out treatment communications from Section 13406.

If HHS believes that some regulation of these treatment communications is necessary, the proposed notice and disclosure model for treatment-related communications represents a potentially viable approach, even if it is not the approach we recommend. This approach will afford patients a meaningful choice in deciding the types of communications they receive, while preserving the ability of providers to deliver clinically significant messages to patients without

first having to go through the onerous step of seeking authorization. We remain concerned, however, that patients will be choosing today to opt-out of future communications about their treatment that ultimately may lead to an adverse impact on their health.

HHS also requested comment on the scope of the statutory exception to marketing (at section 13406(a)(2)(A)), that is, whether communications about drugs that are related to the drug currently being prescribed, such as communications regarding generic alternatives or new formulations of the drug, should fall within the exception of the marketing definition. The Coalition believes a broader interpretation that includes the inclusion of generic alternatives or different formulations of prescribed drugs and related services (*e.g.* injection training for those on insulin) or products that technically may not meet the definition of a generic or new formulation but are intended as a substitute (*e.g.* new mechanism of administration that is clinically justified) should be included in the statutory exception to marketing.

B. Payment Language

We also encourage the Department to include in the final rule an interpretation of the "direct or indirect" language that is used in both HITECH and the HIPAA Proposed Rule. We support the Department's suggestion to use the term "remuneration" instead of the word "payment" in this section. However, there is significant confusion about the phrase "direct or indirect" in the healthcare community. It is important that the Department clarify the meaning of this phrase. We encourage a definition or interpretation of these terms that is consistent with the Department's discussion in the "sale" section of the HIPAA Proposed Rule. Specifically, we encourage a clarification that it is not "direct or indirect" payment for a covered entity to receive reimbursement for its costs in connection with these communications (e.g., when another entity pays for postage or printing costs). This approach would clarify that covered entities need not take a financial loss when making these communications. We also encourage the Department to develop an appropriately flexible standard that makes clear (1) that the payment must come directly from the third party whose product or service is being promoted; and (2) that any "payments" that trigger the authorization must be specifically for making the particular communication, not for associated costs that may be necessary for making the communication, such as development of messages, themes, or other overall program activities (such as development of a wellness program).

5. Sale of PHI

Regarding the "sale" of PHI provision, as discussed in Section 4 above, we encourage retention of the language permitting cost reimbursement, and encourage expansion of the use of this concept into other contexts as well. We understand the rationale for prohibiting the sale of PHI for no other purpose than to profit from it. We are concerned that there are appropriate payments for activities permitted by HIPAA that may be impeded or prevented if this concept is interpreted too broadly. We hope the department will closely review and consider the comments submitted

by the pharmaceutical and biotechnology industries, clinical research organizations and academic health centers regarding this provision.

6. Research

We support the Department's efforts to facilitate valuable healthcare research, through modest changes in the HIPAA Privacy Rule. We support the changes that are proposed by the Department in the HIPAA Proposed Rule. In its modest changes, the Department has addressed specific identifiable problems caused, unintentionally, by the current operation of the Privacy Rule. We support these changes. They will facilitate certain kinds of research activities without affecting patient privacy rights in any meaningful way. In fact, these changes promote patient privacy by giving patients additional control over how their information can be used.

At the same time, we continue to believe that beneficial research activities are being impeded by the current operation of the HIPAA Privacy Rule. We encourage the Department to review additional and broader changes that will permit research on a broader basis. In particular, the Department should review changes that will make it easier for researchers to evaluate health information where primary identifiers have been eliminated (such as with limited data sets) or in other ways where privacy risks involving data are limited. Coupled with the important developments in the health information technology area, there are significant opportunities to improve overall health because of important research, and we encourage the Department to do what it can to ensure that these opportunities are not missed.

7. Minimum Necessary

We understand that the Department is under a requirement from HITECH to provide additional guidance on the minimum necessary rule. At the same time, we are concerned that the approach laid out by Congress is not only confusing but also could lead to significant adverse consequences. Accordingly, while we understand the need for at least some additional guidance, we do not believe that any significant changes need to be made to the minimum necessary rule. This rule operates effectively across the board – it imposes on covered entities and business associates the obligation to evaluate whether data fields can be limited or excluded from use or disclosure; at the same time, the minimum necessary rule does not mandate any specific operational steps. Obviously, despite the HITECH mandate, it is seldom possible for healthcare entities to use a limited data set for most uses and disclosures of healthcare information (*e.g.*, every claim and payment transaction requires individually identifiable information). Accordingly, we have substantial concerns about any effort from the Department to define the "minimum necessary" for any specific activity. We encourage retention of the minimum necessary rule in its current form, and encourage the Department to engage only in very limited guidance on the appropriate minimum necessary steps. The Department should avoid any mandates regarding the use of a limited data set. In addition, the Department should avoid dictating the particular data fields that should be used in any particular context.

8. Self-pay Restriction

We have significant concerns about the operation of the "self-pay" provision of HITECH. We recognize that the Department has identified some of these concerns in its discussion in the HIPAA Proposed Rule. However, we think that the problems raised by this provision are more substantial than those acknowledged by the Department, and we encourage a re-evaluation of this provision.

First, we have substantial concerns about the ability and appropriateness of imposing on providers the obligation to "hide" information about specific claims or treatments across all time periods and all uses of information. We believe that the complexities in this requirement are exceedingly substantial, ranging from compliance with existing contractual provisions (which often preclude charging individuals for otherwise covered services or that dictate specific rates for covered services) to state law reporting issues to follow-up quality control and financial examinations. These challenges may be particularly complicated in certain situations involving integrated delivery systems or other "HMO-like" arrangements where the distinction between provider and payor is not always clear. In short, it may be exceedingly difficult for providers to implement this kind of obligation across all of their activities. Second, and related, we believe that there could be significant gaps in information that is used in connection with health information exchanges and other treatment-related areas, and that this provision may create an additional layer of complexity to all health information exchange efforts. We are concerned that the only way for providers to comply with this provision is to "purge" their records of all information about these treatments, with obvious future risks to patient healthcare. Third, we do not view the Department as having appropriately considered the impact of potential healthcare fraud in this situation. It is clear that this provision, in certain circumstances, will be adopted as a means of supporting fraudulent activities by patients and/or their providers, by hiding relevant information from public and private insurance plans. Therefore, we encourage a review of this provision to incorporate a "best efforts" standard and additional flexibility in the context of fraud investigations or other disclosures where this information is beneficial for other purposes.

9. Access Rights

We understand the Department's efforts in connection with the HIPAA access right. We do not generally disagree with the approach laid out in the HIPAA Proposed Rule – to extend the access provisions of HITECH to all electronic records.[2] At the same time, however, we do not believe

[2] We must caution that while this extension may be appropriate for the HIPAA access right, we believe strongly that it would be wholly inappropriate in connection with the HIPAA accounting right. We have great concerns about the HITECH language about accounting rights even for true electronic health records (where the operating presumption is that this "accounting" function will be automatic), and believe that any extension of these

it appropriate to mandate a shorter time period for the production of this electronic information. We have no substantial concerns with a provision that encourages a shorter response period where feasible, but we object strongly to a provisions that requires a shorter timeframe for production and extends this right to all electronic records.

10. Notice of Privacy Practices

We have significant concerns about the proposed changes related to the privacy notices required by HIPAA. These notices already are exceedingly long and complicated. It is our view that few patients read and understand these notices as currently written. We therefore encourage the Department to engage in a more focused review of the means by which these notices could be shortened and simplified. The HIPAA Proposed Rule, however, moves in the other direction, by imposing additional obligations to add material to HIPAA privacy notices.

We discourage any new additions to the privacy notice requirements, particularly in situations where the primary new requirements relate to areas where the Department has concluded that authorizations are necessary. We do not see the "pro-privacy" value of mandating inclusion in a privacy notice of disclosures that also will require an authorization. This requirement would expand the notices for all patients or members, even where only a small minority will ever be asked for an authorization. Therefore, including these elements will needlessly expand these already bloated notices.

In addition, we do not agree that health plans should be required to issue new privacy notices, as the minor additions do not rise to the level of significant changes related to these notices. We encourage the Department to remove the obligations to insert these new provisions into privacy notices, and to distribute these new notices on a routine basis.

11. Hybrid Entities

In its discussion of section 164.105(a)(2)(ii)(C)-(E), HHS requests comment on whether covered entities that are hybrid entities should be required to include a component that performs business associate-like functions within its healthcare component so that they are directly subject to the rules. We have substantial concerns about this proposal and believe that HHS should not make this designation a requirement. First, we see no need whatsoever for a requirement in this area. Second, and more significantly, we have concerns about the potential implications of this provision, particularly for companies who have "shared service functions" within their company, such as information technology departments, accounting, auditing, legal, etc. We do not think it appropriate to mandate that these departments become – in full – part of the HIPAA covered entity. Instead, covered entities – who must ensure compliance for these functions when

---

principles beyond fully standardized electronic health records could have significant adverse consequences across the healthcare industry.

performing HIPAA functions but not for other functions – should maintain their flexibility to organize their operations as appropriate. Requiring these units to be part of the covered entity in full would either force HIPAA compliance in areas where HIPAA plays no role, or would require companies to create duplicative administrative structures for these functions. We strongly encourage HHS to avoid this new requirement.

12. Compliance Dates

HHS proposes to allow 180 days beyond the effective date of the final rule for covered entities and business associates to come into compliance with most of the rule's provisions. Although we believe that 180 days would generally be an adequate amount of time for most affected parties to achieve compliance with the most of the provisions of these proposed rules, subject to our concerns regarding subcontractors (above), we do not support adopting 45 CFR 160.105, which would create a new default of 180 days for compliance. Current 45 CFR 160.104 provides the compliance default of "no earlier than" 180 days, which has operated successfully for almost ten years now. Compliance with future rules could require two years or more, as was allowed for the initial HIPAA Privacy Rule. We urge HHS to continue to remain flexible with respect to compliance dates for future rulemaking.

Conclusion

The Confidentiality Coalition appreciates this opportunity to work with the Department in the ongoing development of a workable set of rules and guidance in connection with the various HIPAA Rules. We are available to assist the Department in the event there are any comments or questions about the comments in this letter. We look forward to working with you.

Sincerely,

Mary R. Grealy
President, Healthcare Leadership Council
On Behalf of the Confidentiality Coalition

Enclosure

CONFIDENTIALITY COALITION

2010 Steering Committee Membership

Aetna
American Hospital Association
America's Health Insurance Plans
Association of Clinical Research Organizations
Blue Cross Blue Shield Association
CVS Caremark
Federation of American Hospitals
Greenway Medical Technologies
Gundersen Lutheran
Health Dialog
Healthcare Leadership Council
IMS Health
Marshfield Clinic
McKesson Corporation
Medco
National Association of Chain Drug Stores
Pharmaceutical Care Management Association
Pharmaceutical Research and Manufacturers of America
Premier, Inc.
Prime Therapeutics
Texas Health Resources
VHA
Walgreens
Wellpoint

General Membership

ACA International
Adheris
American Academy of Nurse Practitioners
American Benefits Council
American Clinical Laboratory Association
American Electronics Association
American Managed Behavioral Healthcare Association
Amerinet
AstraZeneca
American Pharmacists Association
Ascension Health
Association of American Medical Colleges
Baxter Healthcare
BlueCross BlueShield of Tennessee
Catalina Health Resource
CIGNA Corporation
Cleveland Clinic
College of American Pathologists
DMAA: The Care Continuum Alliance
Eli Lilly
ERISA Industry Committee
Food Marketing Institute
Fresenius Medical Care
Genentech, Inc.
Genetic Alliance
Genzyme Corporation
Health Care Service Corporation
Humana, Inc.
Intermountain Healthcare
Johnson & Johnson
Kaiser Permanente
Mayo Clinic
Medical Banking Project
Medtronic
Merck
MetLife
National Association of Health Underwriters
National Association of Manufacturers
National Association of Psychiatric Health Systems
National Community Pharmacists Association
National Rural Health Association
Novartis
Pfizer
Quest Diagnostics
SAS
Siemens Corporation
Society for Human Resource Management
State Farm
TeraDact Solutions Inc.
Trinity Health
U.S. Chamber of Commerce
Wal-Mart
Wolters Kluwer Health