

September 13, 2010

Ms. Georgina Verdugo
Director
Office for Civil Rights
U.S. Department of Health and Human Services
Attention: HITECH Privacy and Security Rule Modifications
Submitted electronically at <http://www.regulations.gov>.

Re: RIN 0991-AB57, Modifications to the HIPAA Privacy, Security, and Enforcement Rules

Dear Ms. Verdugo:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to submit comments regarding the notice of proposed rulemaking to modify various aspects of the HIPAA privacy, security and enforcement rules in order to implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act. This notice was published in the July 14, 2010 issue of the *Federal Register*.

CHIME's 1,400 members represent chief information officers (CIOs) and other top information technology executives at many of the nation's largest hospitals. CHIME members have front-line experience in implementing clinical systems, and have learned by trial and error what works and what doesn't in implementing such electronic systems and optimizing the value derived from them. Healthcare CIOs share the vision of an e-enabled healthcare system as described by the HIT Policy Committee, the Office of the National Coordinator for Health Information Technology, and the Centers for Medicare & Medicaid Services.

Definition of "Business Associate"

CHIME is definitely supportive of making business associates of covered entities directly accountable for their actions by, for example, providing for the direct imposition of civil money penalties on business associates for violations of the privacy and security rules. We also support the proposed inclusion of various entities in the definition of "business associate," including health information organizations, e-prescribing gateways, other persons providing data transmission services with respect to protected health information to a covered

entity, and persons who offer a personal health record to one or more individuals on behalf of a covered entity.

Definition of “Marketing”

The proposed rule requests comment on the workability of requiring health care providers that intend to send subsidized treatment communications to individuals to provide an individual with the opportunity to opt out of receiving such communications prior to the individual receiving the first communication and what mechanisms could be put into place to implement the requirement. CHIME opposes such a requirement. Among other things, we believe that individuals would even have difficulty in understanding what such an advance communication was all about. In terms of the opt-out option generally, we believe it will be more difficult for providers to track an individual’s opt-out wishes at a service-specific or product-specific level rather than in an “all or nothing” way. Thus, it would appear to be simpler for all concerned to give an individual the option to opt out of all future subsidized communications at the time he or she receives the first such communication.

Sale of Protected Health Information

The proposed rule would require an individual authorization before a covered entity could disclose protected health information in exchange for remuneration (*i.e.*, “sell” protected health information). The proposal includes several exceptions to this authorization requirement.

CHIME understands that an additional authorization would be required, for example, if the covered entity were to sell protected health information to drug companies for their future marketing or for another purpose unrelated to a clinical trial, but we presume that the proposed requirement would not preclude currently authorized activities, such as participation in a research registry in which the investigator and/or coordinator receives funds to pay for the time to compile and enter that data in the registry database or for other study-related expenses or for future use of that registry data. We also seek clarification regarding the exact definition of remuneration, as the impact of this proposal hinges on the exact definition of this term.

In the proposed rule, the Office for Civil Rights (OCR) did not propose to include a restriction on the remuneration that may be received for disclosures for public health purposes but invited public comment on this issue. CHIME sees no need to impose such a restriction with respect to disclosures for public health purposes.

Finally, in terms of remuneration received by a covered entity in the case of disclosures of protected health information for research purposes, the proposed rule requests public comment on the types of costs that should be permitted. CHIME believes these costs should include the cost of extracting and formatting the data (a task that might involve an outside contractor).

Research: Compound Authorizations

In response to concerns expressed by the research community regarding current limits on the use of compound authorizations, OCR proposes to allow a covered entity to combine conditioned and unconditioned authorizations for research (that is, where providers conducting a clinical trial are able to condition research-related treatment on the individual's willingness to authorize the use or disclosure of protected health information for research associated with the trial vs. research activities that cannot be so conditioned), provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. The hope is that the increased use of such compound authorizations would enhance patient recruitment into clinical trials by simplifying the process.

CHIME supports the proposed policy.

Research: Authorizing Future Research Use or Disclosure

The proposed rule indicates that the Department of Health and Human Services (HHS) is considering whether to modify its interpretation that an authorization for the use or disclosure of protected health information for research be research-study specific. This issue is being addressed because the research community believes that the current policy is hampering secondary research. OCR indicates that the following three options are being considered: (1) permitting an authorization for uses and disclosures of protected health information for future research purposes to the extent such purposes are adequately described in the authorization; (2) permitting an authorization for future research only to the extent the description of the future research included certain elements or statements; and (3) permitting option #1 as a general rule but requiring certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities, "such as research involving genetic analyses or mental health records, that may alter an individual's willingness to participate in the research."

CHIME believes the issue should be addressed and that the first option would be the most practical means for doing so. However, we would also note that it will often not be possible to describe future research in as much detail as a current research effort. Thus, researchers should be given reasonable flexibility in describing future research purposes.

Protected Health Information about Decedents

OCR proposes a policy under which individually identifiable health information of a person who has been deceased for more than 50 years would not be considered protected health information under the Privacy Rule. In doing so, OCR indicates that archivists, biographers and historians have expressed frustration regarding the lack of access to ancient or old

records of historical value held by covered entities, even when there are likely few remaining individuals concerned with the privacy of such information.

CHIME is concerned about potential conflicts between what is being proposed by OCR and what state law will permit or require. We ask that OCR indicate in the final rule whether and how state laws that may conflict with the policy would apply. More importantly, we consider this yet another example of how the current HIPAA preemption policy creates problems by essentially allowing geographic variation in privacy rules, which complicates compliance and makes it more costly. We, therefore, urge OCR to re-examine its stance with respect to federal preemption.

Disclosure of Student Immunizations to Schools

The proposed rule would permit covered entities to disclose proof of immunization to schools in States that have school entry or similar laws provided that a parent, guardian or other person acting *in loco parentis* for the individual (or the individual him- or herself if an adult or emancipated minor) provided written or oral authorization. OCR also asks whether the Privacy Rule should require that a provider document any oral agreement. CHIME considers the proposal reasonable and believes that providers would naturally document any oral permission received. Thus, we believe that there is no need to formally mandate such documentation.

Minimum Necessary

OCR uses the proposed rule to solicit public comment on what aspects of the minimum necessary standard covered entities and business associates believe would be most helpful to have HHS address in guidance and the types of questions entities may have about how to appropriately determine the minimum necessary for purposes of complying with the Privacy Rule.

In responding to this request, CHIME would like to begin by emphasizing that any guidance should be broad in nature and continue to provide maximal flexibility to covered entities. OCR also needs to recognize that there are many different purposes for disclosure and that the appropriate way to satisfy the minimum necessary requirement could vary considerably depending on the facts surrounding a particular disclosure. In sum, guidance should remain just that, guidance, rather than an attempt to specify a “one size fits all” policy that could easily conflict with a specific set of facts or circumstances.

Fundraising

OCR emphasizes that an individual should not incur “an undue burden or more than nominal cost” if he or she elects to opt out from receipt of further fundraising communications. In that regard, OCR encourages covered entities to consider the use of a toll-free phone number, an e-mail address, or similar opt-out mechanism that would provide individuals with a

simple, quick, and inexpensive way to opt out of receiving future communications. While CHIME agrees that providers and other covered entities should strive to make the opt-out process easy and simple, we do not believe that OCR's encouragement to do so should be translated into an inflexible regulatory mandate. The circumstances facing a particular covered entity may not warrant or be compatible with a regulatory mandate to use a specific communication mechanism, such as a toll-free number.

OCR also again asks whether the opt should apply to all future fundraising communications or only to a particular fundraising campaign. As noted earlier, we believe it will be more feasible for a provider to track an "all or nothing" decision (after an individual receives the first fund-raising communication) rather than attempt to track the specific type(s) of fundraising solicitations an individual would be willing to receive.

Finally, OCR invites comment regarding possible changes to a current policy under which a covered entity may only use or disclose for fundraising purposes demographic information about and dates of health care services provided to an individual. The proposed rule states that covered entities believe the current policy "prevents them from targeting their fundraising efforts and avoiding inappropriate solicitations to individuals who may have had a bad treatment outcome." For example, the current requirements would not permit a hospital to use cancer diagnosis information to send a targeted fundraising appeal for a new cancer prevention or treatment program to cancer patients and their families. In this regard, the National Committee for Vital and Health Statistics has recommended that covered entities be allowed to use or disclose information related to the patient's department of service (broad designations, such as surgery or oncology), but not narrower designations or information relating to diagnosis or treating physician, for fund raising activities without patient authorization. OCR asks whether the Privacy Rule should allow additional categories of protected health information to be used or disclosed for fundraising or whether the current limitation should remain unchanged.

CHIME urges OCR to retain its current policy and not attempt to enhance fundraising opportunities. We also believe it would be operationally difficult to distinguish between "broad designations" (department of service) and "narrower designations" (diagnosis) since there will be many gray areas.

Notice of Privacy Practices for Protected Health Information

OCR proposes a number of new requirements related to the content of a covered entity's notice of privacy practices (NPP). CHIME is concerned, however, about the growing length of NPPs and seriously doubts that these documents are serving a useful purpose. To begin with, we believe that it would be better for NPPs to focus on issues for which an individual must initiate some action in order to exercise a right rather than inform the individual about every facet of the HIPAA Privacy Rule, including all the obligations that have been imposed on covered entities and their business associates. As the NPPs become longer and longer, we suspect that fewer and fewer individuals even bother to read them, let alone understand them.

Further, in this electronic age, we believe it would be more effective to require that a complete NPP be available on an organization's Web site so that interested individuals could readily access it. Finally, in the interest of administrative simplification, we urge OCR to re-examine the need for patients to acknowledge in writing their receipt of the NPP since this requirement is unnecessarily burdensome and costly. In sum, we consider the current approach to providing NPPs to be both ineffective and wasteful, and we would urge HHS to conduct a thorough evaluation of current NPP policies and practices in order to help identify needed improvements.

Right to Request Restriction of Uses and Disclosures

The proposed rule would require a covered entity, upon request from an individual, to agree to a restriction on the disclosure of protected health information to a health plan if: (A) the disclosure is for the purposes of carrying out payment or healthcare operations and is not otherwise required by law; and (B) the protected health information pertains solely to a health care item or service for which the individual, or person on behalf of the individual other than the health plan, has paid the covered entity in full. This change comes in response to a provision of the HITECH Act. The proposed rule asks for suggestions of methods through which a provider, using an automated electronic prescribing tool, could alert the pharmacy that the individual may wish to request that a restriction be placed on the disclosure of their information to the health plan and that the individual intends to pay out of pocket for the prescription. The proposed rule also requests comment on the obligation of covered health care providers that know of a restriction to inform other health care providers downstream of such restriction. More specifically, the proposed rule requests comment on whether a restriction placed upon certain protected health information should apply to, and the feasibility of it continuing to attach to, such information as it moves downstream. OCR also requests comment on the extent to which technical capabilities exist that would facilitate notification among providers of restrictions on the disclosure of protected health information, how widely these technologies are currently utilized, and any limitations in the technology that would require additional manual or other procedures to provide notification of restrictions.

With respect to e-prescriptions, CHIME does not believe it would be practical to expect the prescribing provider to inform the pharmacy of any privacy restrictions or that the technology for doing so currently exists. The same can be said for communications with downstream providers. Further, the "upstream" provider should not be expected to know whether a patient is truly prepared to pay out of pocket for a prescription or other item or service, especially when both the "upstream" provider and the patient may not even know what the item or service will cost "downstream." One option, of course, unappealing as it may be in an era when policy makers wish to encourage e-prescribing, would be for the patient to request and receive a paper prescription, which the individual could personally take to a pharmacy and there request the same privacy restriction. Another option worth exploring would be for health information exchanges and e-prescribing networks to obtain patient preferences on privacy and authorization directly.

CHIME also believes it is important to emphasize that a patient's information is not totally in a silo. For example, it is very difficult if not impossible for a covered entity to guarantee that information about a certain visit will not appear in another visit's record. Thus, while a covered entity would be able to honor a patient's request not to transmit certain information with respect to a given visit, the same information might well appear in the patient's problem list or on a list of secondary diagnoses submitted as part of a claim for a future service. Given this, we urge OCR to limit the restriction option to a specific encounter with a covered entity, rather than assume it would be feasible to apply the restriction in perpetuity on a diagnosis- or condition-specific basis. We also believe that the narrowest possible policy would be more in keeping with the growing desire to see clinical information shared broadly in order to facilitate care management and care coordination.

In the proposed rule, OCR says that it encourages covered entities to have an open dialogue with individuals to ensure that they are aware that protected health information may be disclosed to the health plan unless they request an additional restriction and pay out of pocket for the follow-up care, and requests public comment on this issue. CHIME believes very strongly that providers should have no routine obligations to discuss potential privacy restrictions with patients. First, this would impose an unreasonable burden. Further, such a discussion would be largely irrelevant to the vast majority of patients and the vast majority of patient encounters. If there is any obligation imposed in this regard, we believe it should lie with the health plans themselves since they have regular avenues of communication with their enrollees. Moreover, health plans could address the issue more efficiently rather than expecting providers to do so each time a visit occurs or a service is provided.

Access of Individuals to Protected Health Information

OCR proposes that if the protected health information is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. In doing so, OCR presumes that covered entities have the capability of providing an electronic copy of protected health information maintained in their designated record set(s) electronically through a secure web-based portal, via e-mail, on portable electronic media, or other manner, but invites public comment on this presumption. Finally, OCR requests comment on whether the provision which allows a covered entity an additional 30 days to provide access to the individual if the protected health information is maintained off-site should be eliminated altogether for both paper and electronic records, or at least for information maintained or archived electronically because the physical location of electronic data storage is not relevant to its accessibility.

First, CHIME believes that the final rule should emphasize that a covered entity's obligation applies only to protected health information that is already maintained electronically in one or more designated record sets.

Second, we note that the timeliness standard under HIPAA is significantly different from that under the electronic health record meaningful use regulations recently adopted by HHS (30 days for information maintained on-site vs. 3 business days). CHIME considers the 3 business day standard unreasonable and is also troubled by the failure to adopt more consistent timeliness standards across HHS regulations.

Third, with respect to information maintained off-site, we would note that even electronic data will be archived to tape or other off-site media and may not be readily accessible. Thus, we recommend against tampering with the existing policy that provides additional time for accessing off-site information. With additional experience, it may be possible to reduce the number of days available for providing access to information maintained off-site, but we believe it would be best to defer a decision about this until some future time.

Business Associates and Covered Entities and Their Contractual Relationships

OCR proposes to allow contracts between covered entities and their business associates to be modified in response to the provisions of the final rule up to one year from the compliance date or 18 months from the effective date of the final rule. While CHIME appreciates the decision to grant additional time for contract modifications, we believe that the proposed amount of time is too short. We urge OCR to provide up to 36 months since many contracts between covered entities and business associates are truly long term. We see little or no value to requiring renegotiation earlier than would be necessary under current contract terms.

Much more importantly, now that business associates will be held directly liable for compliance with the HIPAA Privacy and Security Rules, CHIME questions the need for business associate agreements to recite the HIPAA rules as a vehicle to manage privacy and security compliance. Under the circumstances, maintaining the current business associate agreement content requirement and requiring parties to amend their existing agreements seems unduly burdensome and costly to the healthcare industry. Instead, CHIME recommends that in the covered entity's contractual arrangement with a business associate, the parties be required to (a) define the permitted uses and disclosures required for the business associate to perform its responsibilities, and (b) include a simple statement to the effect that the business associate agrees to comply with the provisions of the HIPAA Privacy and Security Rules that apply to business associates under HITECH. Similarly, as business associates subcontract with parties that are directly regulated under HIPAA as a business associate, a business associate agreement should no longer be required. Rather, the business associate's contractual arrangement with the subcontractor should take the same approach as recommended above. In sum, we believe that the simpler contractual approach we recommend would provide many benefits and substantially reduce the costs of complying with the HIPAA Privacy and Security Rules. This simpler contractual approach described here concurs with a position expressed by the Healthcare Information and Management Systems Society (HIMSS) and we are pleased to endorse that position.

Regulatory Analyses

CHIME is concerned that the costs anticipated by OCR for the implementation of the proposed rule grossly underestimate the real costs the regulation would pose to provider organizations.

Today's electronic records are not architected to establish controls at a granular enough level to enable consumer preference driven disclosure of protected health information. One could reasonably expect that the additional functionality would have the following costs:

One Time Costs

- Vendor software development costs, which will not be trivial, perhaps in the tens of millions of dollars.
- An impact on the volume of transactions processed and logged, therefore requiring further investments in processing capacity as well as storage hardware that could range between a few thousands of dollars per organization, to hundreds of thousands or even millions. One 300 bed facility anticipates an impact ranging between \$250,000 and \$500,000 in hardware upgrades.
- Labor for system configuration and testing required to implement such functionality. One 300 bed facility estimates two to 2.5 analyst level FTEs would be required at a combined cost of \$250,000 to \$350,000 inclusive of salary and benefits to handle this facility's implementation alone.
- Labor and productivity costs associated with training patient access and release of information personnel. One 300 bed facility estimates a training cost of \$20,000 to \$40,000.
- Communications and labor associated with the conversion of current privacy settings for existing patients to consumer driven preferences. One facility with 2 million unique patient records estimates conversion costs ranging from \$500,000 to \$800,000.

Recurring Annual Costs

- Productivity loss to capture and validate consumer preferences at time of registration. One 300 bed facility estimates an added 3 minutes per registration time for 350,000 combined emergency department and outpatient visits and 15,000 admissions per year, meaning an additional \$430,000 in annual labor costs inclusive of salary and benefits.
- Productivity loss to capture and validate consumer preferences at time of release of information. One 300 bed facility estimates an added 15 minutes per release yielding \$60,000 in annual labor costs.
- Annual software maintenance associated with the new functionality.

Assuming 5,000 hospitals in the United States, this yields \$68 billion in one time costs

(excluding software development costs), plus \$2.4 billion annually for the added software-based functionality (excluding annual maintenance). Given all of this, we urge OCR to provide a more realistic assessment of provider and other implementation costs in the final rule.

We hope these comments are helpful. If you have any questions about our comments or need more information, please contact Sharon Canner at scanner@cio-chime.org.

Sincerely,

A handwritten signature in black ink, appearing to read "R. Correll", with a long horizontal flourish extending to the right.

Richard A. Correll, President & CEO