

1730 M Street, NW, Suite 502  
Washington, DC 20036

phone » (202) 659-9440  
fax » (202) 659-9422  
web » www.ahima.org



September 8, 2010

Georgina Verdugo, JD, LLM, MPA  
Director  
HHS Office for Civil Rights  
Attention: HITECH Privacy and Security  
Rule Modifications  
Hubert H. Humphrey Building, Room 509F  
200 Independence Avenue, Southwest  
Washington, District of Columbia 20201

Re: RIN 0991-AB57

Dear Director Verdugo:

On behalf of the American Health Information Management Association (AHIMA), this letter is in response to the Office for Civil Rights' (OCR) notice of proposed rulemaking (NPRM) on "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act" (HITECH) as published in the July 14, 2010 *Federal Register* (Vol.75, No. 134, Pages 40868-40924).

AHIMA is a nonprofit association of over 59,000 health information management (HIM) professionals. These professionals work in a variety of sites that collect, store, analyze, use, and disclose protected health information. HIM professionals have been the stewards of health information's confidentiality for decades and with the advent of the HIPAA privacy and security requirements many serve as privacy or security officers for HIPAA covered entities. AHIMA has supported these efforts over many years and provides members, educators, the healthcare industry, and consumers with a variety of related best practices, and other healthcare confidentiality, privacy, and security information and products. AHIMA also addresses privacy on its myPHR.com website. AHIMA and its member professionals also participate in a variety of privacy-related projects, education, and advocacy on a federal and state basis.

With this background and interest, we were pleased to see the release of these proposed rules and to have this opportunity to comment. AHIMA has solicited comments from our privacy and security experts across the industry including those currently working with health information exchange projects.

As requested, our comments below follow the order in which they appear in the NPRM and we have titled the sections in that order. Proposed sections for which no comment is made signals our agreement with the proposed rule language.

## *II. General Issues*

### *A. Effective and Compliance Dates (75FR40871)*

**AHIMA agrees with the Department of Health and Human Services (HHS) Secretary's (the Secretary) assumption that it is not necessary to extend the compliance date for small health plans.** While split compliance dates may have been required initially for HIPAA transaction standards implementation, we see no reason to segregate this segment of the industry due to revenue size when similar sized provider or business associate organizations are required to meet the initial compliance date.

**AHIMA is concerned, however, with the proposed 180-day compliance period given the significant impact the proposed rule will have on covered entities' manual and electronic systems that are not currently capable of meeting the proposed requirements and for which retooling may not be able to be completed within the 180 day period.** We will comment further on extending this compliance period for some requirements below.

## *III. Section-by-Section Description of the Proposed Amendments to Subparts A and B of Part 160*

### *C. Subpart A-General provisions, Section 160.103 – Definitions: 2. Definition of “Business Associate”*

#### *2a. Inclusion of Patient Safety Organizations (75FR40872)*

**AHIMA agrees with the inclusion of Patient Safety Organizations (PSOs) as business associates.**

#### *2b. Inclusion of Health Information Organizations (HIO), E-Prescribing Gateways, and Other Persons That Facilitate Data Transmission, as Well as Vendors of Personal Health Records (75FR40873)*

AHIMA understands the OCR's desire to simplify the terms used in this section (2.) (b.); however, many different terms are being used to describe HIOs (as noted in the NPRM). **We recommend the final regulation specifies a location on the OCR website where current terms could be listed for any type of transmitting organization that OCR defines as being an HIO and subject to the BA requirements.** There are more terms used by the industry than alluded to in the NPRM and given that it will take some time for the industry to accept a single term we expect questions to continue to arise.

#### *2c. Inclusion of Subcontractors (75FR 40873)*

**AHIMA agrees with the concept of “subcontractors;” however for clarity, we recommend that OCR use the term “business associate subcontractor.”** The term “subcontractor” is often synonymous with “business associate,” in use over the last decade. While using the longer “business associate subcontractor” is also an issue, clarity in this regard is important.

#### *4. Definition of “Electronic Media” (75FR40874)*

AHIMA accepts the changes to the definition of “electronic media.” It has come to our attention, recently, that some copy machines also hold PHI as a result of their use. Just how such data can be accessed and by whom would vary, but it appears that owners of such equipment should come under the HIPAA regulation either by OCR making clear that such equipment should be included in the defined media or, in the case of leased equipment, the vendor should be made a business associate.

#### ***8. Definition of “Workforce” (75FR40874)***

During the introduction of the “Breach Notification for Unsecured Protected Health Information” interim final rule (74FR42740-42770) the issue arose as to who was considered an “agent” of the covered entity. OCR indicated that it took the definition from other federal rules. **AHIMA recommends either defining “agent” in the context of changing this workforce definition, or considering such a definition when OCR releases the final rule on “Breach Notification.”**

#### ***D. Subpart B – Preemption of State Law, Section 160.201 – Statutory Basis (75FR40874)***

AHIMA understands OCR’s explanation with regard to the preemption of state law; however, we must point out on-going concern for the lack of uniform laws and regulations regarding healthcare confidentiality, privacy, and security. As we have previously noted, individuals seeking healthcare do not follow state lines when doing so except for non-emergent care where coverage rules keep them in a single jurisdiction. Healthcare providers, health plans, and other covered entities face even more contradiction as both federal and state governments continue to promulgate conflicting requirements. We urge all policy makers to work toward a nationwide uniform set of rules and regulations and end the confusion and expense of so many variable requirements.

#### ***IV. Section-by-Section Description of the Proposed Amendments to the Enforcement Rule – Subparts C and D of Part 160 (75FR40875-81)***

AHIMA applauds the OCR’s work with the industry and individual entities to educate and make the privacy and security requirements work. AHIMA also believes that it is through strict enforcement that consumers will understand the HIM professions’ and government’s desire to ensure the confidentiality of health records and protected health information wherever it resides.

AHIMA is concerned with subparts C and D of the HITECH provisions and the industry’s ability to comply, given current technology, and while maintaining the need for health information integrity. We will address this further below.

#### ***V. Section-by-Section Description of the Proposed Amendments to Subpart A of Part 164 and the Security Rule in Subpart C of Part 164***

##### ***A. Technical Changes to Subpart A – General Provisions***

##### ***3. Section 164.105 – Organizational Requirements***

##### ***3b. Section 164.105(a)(2)(ii)(C)-(E) (75FR20882)***

OCR raises the question as to whether it “should require rather than permit, as is currently the case under § 164.105(a)(2)(ii) (C), a covered entity, that is a hybrid entity, to include a component that performs business associate-like activities within its health care component so that such components are directly subject to the Rules. **AHIMA believes that any entity that affects or accesses PHI should come under the HIPAA rules both for uniformity as well as clarity of responsibility. Accordingly we believe that OCR should make such components directly subject to the Rules.**

*B Modifications to the HIPAA Security Rule in Subpart C (75FR40882-83)*

We are concerned that the NPRM discussion and modifications appear to suggest that Covered Entities do not need to make as many specific requirements of a Business Associate as in the pre-HITECH agreements because the Business Associate becomes directly subject to HIPAA. **AHIMA believes that Covered Entities should remain concerned with and address the PHI that is created, received, maintained, or transmitted by Business Associates and their subcontractors and not dismiss their (the covered entity’s) obligations to safeguard confidentiality, privacy, and security of their consumer’s PHI.**

*VI. Section-by-Section Description of the Proposed Amendments to the Privacy Rule*

*B. Section 164.501 – Definitions*

*2. Definition of “Marketing” (75FR40884-87)*

In general AHIMA agrees with the changes made in this section; however, we are concerned with requirements where a potential marketing action would require an organization to make changes to its Notice of Privacy Practices (NPP) when the patient segment affected might be a small minority of the total patient population. Instead, **AHIMA recommends that rather than require a change in the NPP, the first defined “marketing” communication contain a clear opportunity to opt-out of future communications and that the method of opting out not be an undue burden to the individual.** Whether or not an organization, especially larger hospitals, clinics, or practices has foreknowledge that it might at some time in the future attempt “marketing” as described in the definition is in many cases unknown. As noted, the target population segment may be small. To require a change in the NPP might be very expensive, yet there may be a benefit to patients to receive such communication. Requiring the first communication to include an opt-out accomplishes the same objective at a much lower cost. Also individuals first receiving an NPP from an organization have little knowledge as to whether they will be subject to such a marketing activity or whether they would potentially benefit. The NPP could note that if an organization initiates a marketing process as defined by HIPAA (HITECH), the individual will be given the opportunity to opt-out.

On a similar note, **we suggest that an opportunity to opt-out clearly apply to the conditions or encounter for which the marketing communication applies.** The patient may be involved in other care where a marketing communication could be beneficial.

*C. Business Associates*

*1. Section 164.502 – Uses and Disclosures and 2. Section 164.504(e) – Business Associate Agreements (75FR40887-89)*

**AHIMA’s concerns with these sections echo our comments regarding the Security rule waiver of contract language which appears to lessen a covered entity’s stewardship obligation for PHI that resides with a Business Associate. Specifically, we do not believe that OCR should remove the obligation of Covered Entities to report Business Associates in violation of HIPAA.** Again we believe that Covered Entities have obligations that cannot be dismissed just because a Business Associate is now covered under HIPAA.

*3. Section 164.532 – Transition Provisions (75FR40889-40890)*

AHIMA agrees with the transition provisions proposed by OCR; however, as we commented above, Covered Entity compliance within 180 days is questionable given current capabilities and technology necessary to meet all of the proposed requirements. Given that additional time is provided for compliance related to Business Associate Agreements, we believe that additional time should also be given for some of the requirements we discuss below.

*D. Section 164.508 – Uses and Disclosures for Which an Authorization is Required*

*1. Sale of Protected Health Information (75FR40890-92)*

In general, AHIMA believes that ONC correctly interpreted Congress’ intent on the exceptions for authorizations; however, we have the following two comments:

With regard to remuneration for preparing, producing, or transmitting data or PHI; the NPRM discusses that the price charged for data “reflect only the costs of preparation and transmittal of the data on research or public health activities including those conducted by or for the use of the Food and Drug Administration.” Later the NPRM adds the term “producing,” and elsewhere in the regulations it is noted that when producing data or PHI for an individual’s request the price charged cannot include the “costs associated with searching for and retrieving the requested information.”

The cost of locating and gathering data reviewing the data for completeness, redacting information to meet requirements for “minimum necessary” or “limited data sets” can be substantial in some cases whether or not the data is electronic. Even with an EHR the data is not always located in one system and HIPAA and other privacy laws require analysis or review of the data before it can be released. In public health, research, and similar aggregations of data the potential redacting of PHI can raise the costs even higher.

**AHIMA recommends that the terms “preparing,” “producing,” and “transmitting” be defined so that organizations can be assured that their pricing meets the requirements established, including any security requirements for encryption or specific media.** AHIMA offers to work with OCR to determine the content of these terms given our 80-plus years experience with these processes.

**AHIMA further believes that the regulation should be rewritten to allow recruitment of all reasonable costs for all activities necessary to prepare, produce and transmit data or PHI as permitted under this section.**

Our second comment deals with the waiver of authorizations when there is a “sale, transfer, merger, or consolidation of all or part of a covered entity and for the related due diligence.” While we understand the reason behind this exception, we note that in these cases an individual’s entire PHI may be involved and individual preference should be accommodated (e.g. the patient might not want his or her PHI to be possessed by the new entity.). **AHIMA recommends that OCR consider this issue and provide an interim final rule that addresses how an individual might be contacted and given the option of such a transfer.**

## *D.2. Research*

### *2b. Authorization Future Research Use or Disclosure (75FR20893-94)*

AHIMA supports the OCR’s willingness to address authorizations for future research use or disclosure. We support OCR’s moving forward to consider Option 3 which takes into consideration genetic research and similar activities while recognizing that the detail in Option 2 is not always available at the time an authorization is sought to the extent that OCR appears to desire. Revocation especially in large organizations can be difficult, but we believe that registries can be developed to track research information and data, and the cost of such registries must be borne by the research projects. **AHIMA suggests that in addition to this issue being addressed by the HHS Office for Human Research Protections and the FDA, that the National Committee on Vital and Health Statistics (NCVHS) also be involved so that there can be a full industry discussion with the panel entrusted to make recommendations with regard to HIPAA privacy and security.**

## *E. Protected Health Information About Decedents*

### *1. Section 164.502(f) – Period of Protection for Decedent Information*

AHIMA members could not reach a consensus to support the recommendation of the OCR for a limit of 50 years for decedent PHI. Concerns and examples were raised that suggest that either the rule be kept as it now stands, or a mechanism be devised for the individual to indicate their desire to have PHI lifted after 50 years. We have no information on how consumers would relate to such a question, but we recognize an exception would create an increased administrative burden. We also note that there are state laws that may require an entity to protect such information beyond 50 years and there are numerous reasons why some healthcare providers keep records for a longer period.

### *E2. Section 164.510(b) – Disclosures About a Decedent to Family Members and Others Involved in Care (75FR40895)*

HIM professionals fully understand care givers or family members need for information concerning a decedent; however, it is extremely difficult, especially in hospitals and other facilities to determine just who fits the description of “involved in care” and “family members.” **AHIMA requests OCR be more specific in its definitions of “involved in care” and “family members.” Further, we suggest that those with “medical power of attorney,” “power of attorney,” or the deceased’s estate executor be added to this list.** While we realize that the individual’s clinician often can identify such individuals, this is not a practical solution. The additional definition requested would be extremely helpful so that administrative staff might inquire at admission or during an individual’s admission.

*F. Section 164.512(b) – Disclosure of Student Immunizations to Schools (75FR40895-96)*

AHIMA supports OCR’s inclusion of immunizations to schools as a public health disclosure. Ongoing testimony to the NCVHS pointed out the difficulty that school officials had in obtaining such information.

**AHIMA recommends that covered entities record oral authorizations in the patient’s health records including the date, name of the individual’s parent, guardian or emancipated minor authoring the release and the name of the individual and school (and address) to which this information is to be released.** A substitute form containing the same information along with the name of the subject individual could be used for face-to-face communication. Most immunization records are held by local physician practices or clinics that are familiar with the local schools; however, given other requirements included in the HITECH privacy legislation and this NPRM, **OCR should define appropriate means of submitting immunization records between the practitioner and the school so that both parties are comfortable with the exchange and confidentiality can be maintained.** For instance, should such information be sent electronically and encrypted?

The NPRM discusses how PHI is protected by the Family Educational Rights and Privacy Act (FERPA) once it is received in the schools. AHIMA notes that the NCVHS has held several hearings in which testifiers have noted that access to such student health information or PHI is much more lax under FERPA. **AHIMA urges OCR and HHS to work with the US Department of Education to tighten FERPA’s requirements in order to offer more confidentiality than is currently available and be consistent with HIPAA/HITECH.** There is generally no need for information, such as immunizations, to go beyond school clinicians as currently permitted by FERPA.

With regard to the definition of “school;” AHIMA suggests the term “school” apply to any state or local licensed school, public or private, open to children from birth to 18. While we recognize that secondary schools might service adults age 18 and above, we also believe that in these situations the usual process of obtaining an authorization should be followed since the patient is an adult.

*G. Section 164.514(d) – Minimum Necessary (75FR40896)*

Generally, our members were comfortable with the current “minimum necessary” requirement. Providers (covered entities) had some concerns that health plans push occasionally on some requests and believed that the existing regulations could make the point more clearly regarding the healthcare provider’s stewardship role in ascertaining what is “minimum necessary,” since the existing HIPAA rule permits the health plan to define what it believes is “minimum necessary” often creating conflict with the healthcare provider. These individuals noted that often a healthcare provider cannot get paid unless they provide what the health plan requests either as part of the claim process or in a chart audit.

Members also note that there is a pending CMS final rule on HIPAA “Attachment” standards which, if it follows the current CMS NPRM approach would violate minimum necessary since one of the alternatives opens provider electronic records to direct access by health plans for payment purposes. Attachments are addressed by Patient Protection and Accountable Care Act (PPACA) and will be addressed by the NCVHS. AHIMA recommends that as OCR considers minimum necessary it should include a prohibition on health plan access to an individual’s PHI under guardianship of a healthcare provider.

**AHIMA suggests that OCR, ONC, and CMS consider a requirement for “minimum necessary” access in systems under a future stage of “meaningful use” certification.**

Minimum necessary also applies to a covered entity’s workforce access to PHI. Many EHR vendors do not design screens or access software that limit information on an individual to what is necessary for the task at hand, defined either by the location of the access or the permission granted the workforce member. While there is no thought to limiting information for clinicians, there are many non-clinicians who normally do not need access to all of the data or the record. Some existing software products do not give covered entities as much leeway to limit access as they would like for compliance and few systems offer a package that would allow a covered entity to provide an individual with a read only access to his or her EHR.

***H. Section 164.514 (f) – Fundraising (75FR40896)***

AHIMA agrees with OCR’s approach to providing an opportunity for individuals to opt-out of a facility’s fundraising effort and the concern that such a process should not cause undue burden on the individual. We do not see a reason to first seek permission (opt-in) from the individual before starting a targeted fundraising effort as long as an easy option to opt-out is provided.

***I. Section 164.520 – Notice of Privacy Practices for Protected Health Information (75FR40897-98)***

With regard to the notice of privacy practices questions, AHIMA has the following comments:

**Breach: AHIMA agrees that the NPP should provide a statement regarding its responsibilities associated with a breach of unsecured protected health information. AHIMA urges OCR to finalize the notification of breach requirements so that a covered entity’s NPP could be updated just once as related to these regulations and the pending breach regulations.**

- **Health plan NPP:** AHIMA members note that many health plans now communicate with subscribers via e-mail and similar electronic communications or by regular mail. Many health plans also have web sites. Therefore, **AHIMA suggests that health plans be directed to notify subscribers of their revised NPP in their next communication after the 60-day period and direct subscribers to either a website where the NPP can be downloaded or other non-Internet options. Health plans could then have the option of notifying all or all remaining subscribers in their next annual mailing; therefore, covering all subscribers at a limited cost. Should a health plan not be able to communicate in these ways, then the rule should require the health plan to notify subscribers within the initial 60 days. Separate notification should be permitted by post card pointing subscribers to either download the new NPP at a website, or contacting the health plan for a separate mailing if desired. OCR and HHS could assist in this effort with public service announcements that would urge consumers to visit their plan website for more information.**
- **Providers NPP:** We believe posting a new NPP and publicly asking individuals to inform the provider if they desire a copy would be the appropriate option from among those suggested.
- **Written Acknowledgement:** Currently § 164.520(c)(2)(ii) requires that “except in an emergency treatment situation, [a provider must] make a good faith effort to obtain a written acknowledgement or receipt of the notice...” **OCR should eliminate this requirement given the experience of the initial NPP acknowledgement requirement, which our members indicate made limited sense to most consumers, had little return except when the NPP was presented in person, and resulted in a collection of paper forms that had limited use for anyone.**

*J. Section 164.522(a) – Right To Request Restriction of Uses and Disclosures*

AHIMA members have many concerns with this section and given the NPRM requests such concerns, they are listed below.

**General concerns specific to the request for restriction:**

**While AHIMA members replied from the various perspectives of providers who use paper-based, hybrid, or a variety of electronic health record systems; all respondents indicated significant concerns regarding the ability of a provider to accept the restriction and their ability to accurately meet the requirements of this right. AHIMA members note that it is very likely that few individuals will request such a right, as a percentage of the total patient population, while the attempt to build any process or system to respond to this requirement will be costly for all. Members also note that this requirement will affect all of an institution’s systems associated with patient care as well as the systems of all professionals who treat the individual (whether or not they provide the direct service or item) on an on-going basis associated with the organization and follow-up care. There is also concern that**

**in restricting information for payment, the availability and integrity of information for continued clinical care may be compromised.**

**Other general comments include:**

- **Timing of a request for restriction:** There is no clear point at which a patient might, or must, determine his or her desire to pay for an item or service, unless it is an item or service that they are aware they will be receiving as they enter the provider (such as specific elective services). The HITECH requirement would therefore require all staff who interact with a patient to be trained and have access to a process or system that would enable the staff member to counsel the patient on the decision and communicate with a variety of other staff who must facilitate such a request (e.g. registration/admission, cashier, business office, ancillary office, offices of professionals who bill separately (in a hospital or large clinic), and so forth.) While it has been suggested that EHR systems could be changed to process only at discharge, this would not be efficient or effective for admissions and for systems with intelligence capabilities that are designed to interact with the clinician during the encounter.
- **Timing of request:** Often there are a number of services that might be associated with the particular item(s) or service(s) the patient may wish to restrict from the health plan. These services may or may not be obvious to the staff member who is counseling the patient at the time of the patient request, and the patient may not wish to pay for these associated services which will trigger information that would in fact signal the health plan that information was restricted. To meet this requirement may require some unbundling of services in the administrative systems, which will also be costly.
- **Timing of request:** Patients will be required to make any declaration of a request and payment at the time of service. Many providers of outpatient or ambulatory services do same day billing, so any delay in their process will increase their accounts receivable and limit an individual's time in which to make a request.
- **Timing issue:** Some long-term patients may not be capable of requesting a restriction in time to prevent a claim since the facility may process an interim bill which includes such a service.
- **Administrative and clinical processes:** The requirement allowing a restriction of a service or item will mean that the associated classification coding and other information associated with the services must be flagged in such a way (in paper or electronic environments) so that any follow-up transactions associated with this encounter or subsequent encounters with a health plan do not inadvertently provide the restricted information. In addition, health records or EHRs will have to be scrutinized and redacted when providing records to health plan auditors (such as the RAC program), and any request for PHI associated with the encounter or admission where the restriction was requested in order to ensure compliance. Note, this is an additional activity in the release of information process that will add to the cost for an administrative service that may not be remunerated by a ROI fee as described in this NPRM.

- **Clinical impact:** Services and items are often recorded in physician or other clinician notes. To meet this NPRM requirement any reference to the service or item will require redacting of information in clinician notes should they be required for the reimbursement of other services by the health plan. Such redaction will, of necessity, require review by clinicians and redaction will be potentially obvious in many cases to the health plan. This same redaction process will be required for any audit by the health plan.
- **Consumer question:** Should a complication occur due to the restricted service or item and the patient not desire to cover the costs of treating the complication, how can a provider bill these costs and not inform the plan of previous services?
- **Consumer question:** Patients and staff will need to be reminded of this restriction for each encounter or admission since the same process will have to be followed unless the patient lifts the restriction which could then alert the health plan to the previous restriction.
- **BA involvement:** Many providers use business associates to do billing, ROI, and other administrative tasks associated with meeting this requirement (such as payment collection or “self-pay” billing); however, the NPRM suggests that BAs should not be permitted to handle this restricted information, causing providers to set up systems they would not normally use.
- **Technical issues of splitting charges:** While organizations generally have a “self-pay” category for a patient, most administrative systems and clearinghouses do not have an application that allows for splitting charges within a single encounter. To honor this proposed requirement and tie it to specific procedures and possibly diagnosis codes will be both time consuming and expensive. The only groups that we identified that can split an ambulatory encounter are small physician offices not engaged in electronic billing and some student health centers.
- **Technical Issue – lack of systems:** While paper-based systems might permit flagging a request in the master patient index the associated process would have to be manual throughout. **Our members are not aware of EHR systems that currently can accommodate this requirement, and do not believe such systems will be available for implementation in the 180-day limit for compliance.** Again these manual processes and additional systems add to the cost of healthcare and perhaps dictate that a fee be permitted to cover the handling of such requests except when the individual pays for the entire encounter or admission and not just the service or item. Even then there will be costs to ensure that information does not leak to the health plan in the future (as noted above).
- **Technical Issue – Overlapping implementation expenses:** Provider organizations are currently implementing changes to the HIPAA transaction standards which affect these same administrative applications; therefore potentially doubling the expense organizations will encounter within the same time period (2010-2011).
- **Technical issue:** Organizations may wish to go back to paper billing or build a new billing system from scratch to accommodate such a restriction practice – technically under today’s reimbursement and claims systems this requirement is not feasible.

**E-prescribing (75FR40899):**

- **Up-front request for restriction:** Many larger organizations and even mid-size healthcare clinics and practices are engaged in e-prescribing including the use of hand-held devices to initiate prescriptions. In some cases prescriptions may be written throughout an encounter. Many providers do not use an internal pharmacy in ambulatory situations, preferring to send prescriptions to the patient's identified private pharmacy. Providers will have to notify patients of their need to inform their physician or other clinician (at the beginning of an encounter) if they desire to pay out of pocket for any prescription. This action would be needed at the beginning of each encounter with each separate clinician (since there may be many involved in an encounter).
- **Similar impacts:** It should be noted that this same requirement of clinician notification would be necessary for clinicians using CPOE for ancillary services requests where an individual desires to pay for the service or item.
- **Dual paper and electronic prescribing:** Some organizations expressed concern that requiring physicians or clinicians to use both electronic and paper prescription systems or forms is counterproductive to their attempt to go electronic.
- **Quality measure and other reporting:** Concern was raised that quality measurement reporting requirements could provide a health plan with an indication of the restricted service or item.

**Informing other health care providers downstream of restriction (75FR40899-40900):**

- As noted, many responders are concerned about just how (and when and if) to communicate with clinician providers who bill separately but are involved in the same encounter or admission of the patient as a provider or consultant. While AHIMA believes it is appropriate to share the individual's restriction request with clinicians involved in the facility's care, **AHIMA does not believe that it should be a covered entity's responsibility to notify downstream providers (those not associated with the specific encounter or admission) of the restriction. This should be the responsibility of the patient.**
- Members have also raised concerns that it may be necessary to share clinical information in health information exchange organizations (HIEOs). This presents a dilemma similar to that of downstream providers since there is no standard means of flagging such information at present. If such information were to be flagged, electronic health records systems and HIEO would have to adhere to a standard and individuals would have to be apprised that their "flagged" information would be shared.
- Given that HIEOs and similar organizations are now considered business associates, and given that OCR has suggested that healthcare providers are not permitted to share such plan-related restricted information with business associates (75FR40899) some of these concerns may be moot, however, this then puts healthcare providers in the situation of providing less than the PHI that may be necessary for a requested transmission of clinical information through a HIEO (BA). As noted the restricted PHI may be in physician or other clinician

notes. **AHIMA believes that it would be inappropriate to redact such notes when provided to another provider and flagging such notes to reflect such a restriction would be difficult.**

**Disclosures to health plans that may be “required by law” in spite of the individual’s restriction (75FR40900):**

- Members are aware of some potential situations where information may be required to be submitted under state laws. **We recommend that such situations be exempted from this HITECH provision and the individual be notified of such either in the NPP or individually when a request for a restriction is made.**
- Members are very concerned as to how these HITECH requirements affect individuals covered under Medicare or Medicaid and other federal or state programs that require providers to bill in full. We did not see any legislative or regulatory language that addresses this conflict, and members point out that failure to provide the information as required by these government health plans could place the provider in a position of being accused of false billing. On a similar note, most workers’ compensation programs are exempted from HIPAA but carry state requirements requiring identification of all services and items. Failure to provide such information to these programs could put providers in a position contrary to state law. **AHIMA requests OCR to address this issue and clarify how such providers are to respond to the requirements of HITECH and government programs. If HITECH requirements supersede government health plans then providers should also be permitted to redact records going to other government programs such as RAC auditors.**
- Members also note that many health plan contracts currently require either claims information or audit information that might identify the restricted service or item. This will require an amendment to provider-health plan contracts. **AHIMA recommends that OCR add a requirement that no health plan provider contract or process require the provider to violate this HITECH provision being added to HIPAA.**

**HMOs (75FR40900):**

- Discussions with AHIMA members echoed the NPRM concern that HMO members desiring a service or item that they did not want reported to the HMO would have to go out of network under current HMO laws or contracts. Out-of-network encounters would have to be covered by the individual unless they have primary coverage with another payer and the HMO might be considered secondary where the individual could then fail to note the HMO as a secondary payer. In some communities it may also be difficult for patients to seek out-of-network care.
- AHIMA members further note that if out-of-network care is paid for and received by the patient, the clinical data from that encounter will be missing from any longitudinal records unless the patient permits or themselves provide such information to the HMO provider.

Such a provision of clinical data could negate the restriction in the future as expressed in some of our other comments.

**Payments not made in full or “bounced” payments (75FR40900):**

- Members suggest that the ability of the healthcare provider to lift the restriction in cases of “bounced” payments should be indicated in any NPP or other communication with individuals seeking to restrict information from reaching their health plan. These members believe that such a notification will be a significant deterrent.
- These members also note, however, that such “bounced” payment issues further complicate the billing and “credit” functions of the provider adding additional cost and therefore in these situations providers should have the option of adding a fee. Members also point out that these situations are often handled by business associates and if OCR does not permit business associates to handle these situations then providers will have to build in-house systems adding significant administrative expense.

**Restrictions when there is follow-up care (75FR40900-01):**

- AHIMA agrees with OCR’s approach to follow-up care situations where no restriction is requested but to be reimbursed the provider must provide restricted information from the previous encounter. The counseling that OCR suggests raises the issue of who should do such counseling, how they will know such counseling is needed, and whether it is appropriate to include a written statement to the individual letting them know of these repercussions for any potential follow-up care. If a flag could be raised on a second visit, it might become the role of administrative staff, however, as pointed out elsewhere in the NPRM, the individual may not be prepared, or able, to cover the cost of the second visit

**Specific concerns with regard to these requirements (75FR40899-40901)**

As noted our HIM professionals have a number of concerns related to this restriction, which have been laid out above; however there are a few concerns that we feel need emphasis:

- We are concerned that currently there are few administrative and clinical systems that can handle this requirement internally let alone externally. **If this requirement cannot be amended, then AHIMA recommends that this requirement be delayed until the necessary standards, certifications, and software products that can handle this requirement are available and can be implemented across healthcare administrative and clinical systems while maintaining data integrity and providing continuity of care as well as meeting similar patient clinical needs.**
- **As noted, we are concerned that providers’ attempts to meet these requirements will impact clinical data integrity as well as administrative data and secondary data.** Many providers are not sophisticated enough, at this time, and do not have the technical capability to process health information and function under this requirement. In addition there are many secondary uses of clinical data beyond reimbursement that require information that the

patient wishes restricted. **If the redaction is not handled correctly, the data integrity for these other uses and perhaps in some cases treatment requirements will be in jeopardy.**

- Providers are fearful of not meeting the compliance requirements for this HITECH privacy provision since conceivably any workforce member, including physicians or clinicians (who may not be considered a workforce member) dealing with the individual must be prepared to work with this restriction process. With so many workforce members and information systems involved, our HIM professionals fear that it will be easy to become non-compliant.
- As noted, members are also concerned that while they may be compliant with this HITECH requirement, there will be allegations of fraud with regard to relationships with a variety of government programs and potentially some private healthcare programs as well since information will be withheld. **HHS must define how providers can be compliant with various federal (and state) government programs that will have conflicts with the request for restrictions when government is the health plan.**
- As noted, business associates are deeply involved in the processes that might accommodate a restriction. **We believe that OCR should allow business associates access as needed.**
- Healthcare providers are unique as businesses since in most cases they bill third parties for services rather than the patient. This practice existed as a convenience to the patient or subscriber and administrative and clinical systems have been developed to work with this process. While HIPAA shared the confidentiality requirement for healthcare among providers and health plans, taking the health plan out of the equation presents many of the problems cited above and this HITECH requirement conceivably could be cost prohibitive for large organizations in the short term (2010-2016). Such costs will increase the overall cost of healthcare for all consumers to the benefit of only a few. We doubt that the average patient can afford a fee that would cover the administrative costs involved. None-the-less, **we believe that some fee should be charged to handle these exceptions.**
- We asked members for alternatives that would allow providers to meet the issue we believe Congress was trying to address. **We could only come up with requiring the restriction apply to the full encounter or admission, even as you note this presents some problems. We believe, however, that the cost of such an approach would discourage some individuals and be appropriate for their reasons in the first place. As noted, moving an entire encounter or admission to “self-pay” also is much less costly to organizations. OCR should reconsider its prohibition of this alternative.**

*K. Section 164.524 – Access of Individuals to Protected Health Information (75FR40901-03)*

**Overview**

The current environment of covered entities is extremely mixed when it comes to having EHR systems as described in this section. While there are a number of organizations who would be considered as having a fully electronic record, others are in a paper-only situation, and most are in a hybrid mode moving from paper to electronic in steps and stages.

With the exception of some physician practices most providers do not have a single software application that encompasses their EHR, rather they have a number of different systems whose collective information provides an EHR from which information can be obtained for clinical care and a variety of secondary purposes. The ARRA-HITECH incentive program, which is voluntary, calls for an organization to be able to provide certain amounts of information in a data set defined under standards adopted by HHS. These data sets are only a subset of data and not the data or information that makes up the “complete” record collected from the various subsystems.

The NPRM appears to appreciate the complex nature of the EHR and the fact that at this time there is no universal agreement on what constitutes the complete or “legal EHR.” The NPRM also appears to understand that access to the record under the HITECH requirements is in fact access to a copy of the record. Since the “record” might reside in different systems, such a copy – if the entire record is desired – may have to be a compilation of the various paper and electronic records.

EHR systems, for the most part, have not been developed for a consumer to have access (review) of an entire record on-line. Screens have been developed for various other users, generally clinical and administrative staff. To give an individual “access” to their record becomes difficult unless the components of information associated with an encounter(s) or admission(s) can be analyzed by trained staff (e.g. HIM professional). Since this is the case and since there are no universal standards across all components that make up an EHR system, members report that they can either provide the individual with copies of certain segments of the electronic record (like that required under Meaningful Use which will be developed using a standard) or a manual process to produce a CD in “PDF” format from the electronic and scanned paper documents.

While “patient portals” are gaining popularity, they are still offered by relatively few healthcare providers or health plans, and when offered the information available is defined by the organization offering the portal. Our discussions did not surface any organization whose portal would display anything close to a full record.

For security purposes AHIMA members report that most organizations would prefer to produce a CD in PDF format or a covered entity provided flash drive. Organizations are uncomfortable allowing individuals to attach their personal flash drives to the organization’s system for security purposes. Covered entities are also concerned with regard to the security of sending information via e-mail without some sort of security protocol acceptable in the industry and by consumers.

### **Specific Responses**

- **AHIMA believes that all consumers (with rare exception) should have access to their PHI and the ability to request a copy of their PHI.**
- **Form and Format:** While AHIMA members accept the need for discussion on the electronic form and format requested by the individual, in fact, form and format will be dictated by the covered entity’s system unless the PHI requested is a standard format such as those required under Meaningful Use, and given the current environment of systems and

paper in the healthcare industry most output will of necessity be in PDF format on a CD or covered entity-provided flash drive. AHIMA and its members are actively working toward standards-based EHRs and interoperability that in the future will permit a smoother delivery of health information across the healthcare spectrum including to patients. With this in mind, **AHIMA agrees with OCR that the form and format have to be discussed between the individual and the covered entity.**

- **Patient Portals:** AHIMA members' organizations are in the midst of considering or establishing patient portals that may provide consumers with adequate information and communication regarding their healthcare and PHI. There is no uniformity in these portals, but we urge HHS to consider whether some uniformity might be appropriate in the future as opposed to information being pushed from covered entities to consumers. Some covered entities are sharing information with third-party patient health record (PHR) organizations, but there is a desire for uniform security and data standards in transmission with such organizations.
- **Security:** AHIMA members believe that the same security requirements should be in force to mail an electronic copy of an EHR or PHI information (on a CD or flash drive) as currently is in place for paper copies and suggests that all such information should be encrypted, unless presented in-person to the individual or their representative with a specific request to not encrypt. AHIMA does not recommend that covered entities be forced to accept a consumer's flash drive for downloading of PHI, due to security concerns; however, the cost of flash drives (to be provided by the covered entity) is fairly nominal and should be covered.
- **Response Times:** AHIMA notes that there are specific response times in the Meaningful Use criteria that may or may not conflict with those required under HIPAA. When there is a specific data set standard and the covered entity has the electronic record data that makes up this data set, a shorter time period than that required under HIPAA may be doable; however, as noted many covered entities are in a hybrid situation, and the industry does not have a standard for the electronic health record that may be requested by the consumer. Therefore, while AHIMA is working with its HIM members and the industry to achieve a real time fully functional and legal EHR, at this time **AHIMA must recommend that the response times for consumer requests remain as currently stated under HIPAA.** At the same time AHIMA urges covered entities to establish systems and processes to better enable access to PHI.
- **"Access" to PHR Fees/Copy Fees:** As noted elsewhere in our comments, the task of gathering information to provide a copy of PHI or the EHR varies greatly. If there were a standard EHR system and if every provider had such a system, then the concept that responding to a request should only be the cost of the media and the transmitting or mailing makes sense. That is not the case now where some information can directly be provided while other information must be collected and scanned to produce a copy in some form that an individual might understand. In addition, as pointed out in the NPRM custodians of the PHI or records must take steps to authenticate the request and requestor as well as arrange a secure method in which to provide the PHI. **AHIMA agrees that fees for such activities**

**must be reflective of the actual costs; however, AHIMA also believes that all of the actual costs must be reflected in the fee or the cost will be assumed by all of the consumers of healthcare or healthcare products at that covered entity. AHIMA urges OCR to recognize and permit all reasonable labor, material, and capital costs to be recovered in fees to produce PHI today.**

- **Transfer of PHI/EHRs to third parties:** AHIMA members agreed to the NPRMs approach to sending PHI/EHR copies to third parties when the individual or personal representatives make the request themselves and provide the information required. Again the process of sending copies of the records to third parties has created concerns in the past with regard to the cost of recovering the labor etc., associated with creating this copy, as discussed several times above.

Because of the volume of requests and the labor involved many healthcare providers engage ROI vendors to search their records and provide the requested PHI. The potential of this NPRM prohibiting BAs from handing PHI would prohibit this process and require covered entities to take on the task internally potentially raising cost and creating a large backlog of requests. **AHIMA asks OCR to allow business associates to work with such information as required by covered entities.**

AHIMA appreciates the work that the OCR and other HHS staff have undertaken to produce the July 14 NPRM on HITECH Privacy changes, and the work and effort that will be required to review these and other comments to the NPRM. We appreciate the opportunity to comment on these proposed regulations and commit to responding to any additional inquiries OCR might make and to working with the OCR in any way possible to secure and protect PHI wherever it may lay or through whatever means it may be transmitted.

If there are additional questions or concerns regarding this response, or other questions with regard to HIPAA, HITECH, or confidentiality, privacy or security, please contact me at the address or phone number above, or at [dan.rode@ahima.org](mailto:dan.rode@ahima.org). In my absence, please contact either Allison Viola, AHIMA's director for federal relations, at the same address and phone, or at [allison.viola@ahima.org](mailto:allison.viola@ahima.org), or Harry Rhodes, AHIMA's director for practice leadership at (312) 233-1119, or [harry.rhodes@ahima.org](mailto:harry.rhodes@ahima.org). We thank you for your time and consideration of these comments.

Sincerely,



Dan Rode, MBA, CHPS, FHFMA  
Vice President, Policy and Government Relations

Cc: Allison Viola, MBA, RHIA  
Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA  
AHIMA Membership  
Office of the National Coordinator