



230 E. Ohio Street, Suite 500  
Chicago, IL 60611-3269  
Tel 312 664 4467  
Fax 312 664 6143

[www.himss.org](http://www.himss.org)

The Honorable Kathleen Sebelius  
Secretary  
U.S. Department of Health and Human Services  
200 Independence Avenue, SW  
Washington, DC 20201

Ms. Georgina C. Verdugo, JD, LLM, MPA  
Director  
Office of Civil Rights  
U.S. Department of Health and Human Services  
200 Independence Avenue, SW  
Washington, DC 20201

Dear Secretary Sebelius and Director Verdugo:

On behalf of the Board of Directors and members of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to submit written comments on the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) Notice of Proposed Rule Making (NPRM) on proposed modifications to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Enforcement Rules ("HIPAA Rules") published July 14, 2010 (75 Fed. Reg. 40868).

HIMSS is a cause-based not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare. Founded 50 years ago, HIMSS and its related organizations have offices in Chicago, Washington, DC, Brussels, Singapore, Leipzig, and other locations across the United States. HIMSS represents more than 30,000 individual members, of which two thirds work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes over 470 corporate members and more than 85 not-for-profit organizations that share our mission of transforming healthcare through the effective use of information technology and management systems. HIMSS frames and leads healthcare practices and public policy through its content expertise, professional development, and research initiatives designed to promote information and management systems' contributions to improving the quality, safety, access, and cost-effectiveness of patient care.

HIMSS appreciates the opportunity presented by OCR to comment on the important privacy and security modifications under the Health Information Technology for Economic and Clinical Health (HITECH) Act. We share OCR's vision that national standards for the protection of privacy and security be required of all covered entities (CEs) and their business associates (BAs) and believe that the HIMSS goal of health information technology (HIT) adoption is best achieved through strong privacy and security protections. We also recognize that HITECH envisions a complex and highly interrelated regulatory scheme to support electronic health record (EHR) adoption for improved quality, safety, and efficiency, reduced health disparities, and improved care coordination, population and public health activities, and patient engagement.



Response to Office of Civil Rights (OCR) Notice of Proposed Rule Making (NPRM) on proposed modifications to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Enforcement Rules (“HIPAA Rules”) published July 14, 2010 (75 Fed. Reg. 40868).

HIMSS solicited comments from its members and leveraged special subject matter expertise through collaboration between our Legal Aspects of the Enterprise Task Force and Privacy and Security Committee. In particular, HIMSS wishes to comment on the following areas:

1. The necessity and utility of continuing to require Business Associate Agreements (BAAs) to manage privacy and security compliance now that Business Associates (BAs) are regulated directly under HITECH
2. The BA definition, the definition of “conduit” and “health information organization” and the extent to which the conduit exception applies
3. The urgent need for OCR guidance under the minimum necessary standard
4. The effective date and the compliance date of the final rule

In the interest of ensuring the government has access to other relevant comments from the HIMSS membership, member comments on specific line items in the NPRM are provided as Attachment #1 to this letter.

With respect to items 1-4, HIMSS offers the following comments:

**1. HIMSS believes the direct liability for HIPAA imposed on business associates under HITECH obviates the need for covered entities and business associates to enter BAAs that recite the Rules as a vehicle to manage privacy and security compliance.** Maintaining a BAA requirement under the HITECH Act is unduly burdensome and costly for the healthcare industry. Instead, HIMSS recommends that in the covered entity’s contractual arrangement with the BA, the parties be required to (a) explicitly define the permitted uses and disclosures required for the BA to perform its responsibilities, and (b) include a simple statement affirming that the BA agrees to comply with the provisions of the HIPAA Privacy and Security Rules that apply to business associates under HITECH.

The HITECH Act dramatically shifts how business associates are regulated. Before the HITECH Act, business associates were not directly subject to either the Privacy or Security Rules. OCR could not investigate, penalize or recommend for prosecution any BA who had violated a provision of the Privacy or Security Rules. Any attempt to enforce HIPAA requirements by fine or prosecution could be applied only to covered entities, and the only mechanism to hold business associates responsible for violating the Privacy or Security Rules was the BAA.

The HITECH Act changes this statutory requirement and expresses a clear policy that business associates are to be held accountable for their actions. Under the HITECH Act as implemented by the NPRM, business associates (and their subcontractors) will now have direct liability for compliance with the HIPAA Privacy and Security Rules and will be subject to the same criminal and civil penalties applicable to covered entities that violate the Privacy or Security Rule. Therefore, it is no longer necessary to require BAAs that recite the HIPAA Rules as a vehicle to manage privacy and security compliance.

Requiring covered entities and business associates to affirmatively amend their BAAs under HITECH places an undue burden on the health care industry that will impede efforts of covered entities and business associates to focus on best practices and other substantive privacy and security policies and procedures. The changes we have outlined would lower the cost of compliance and simplify the administration of privacy and security compliance. Similarly, as business associates subcontract with parties that are directly regulated under HIPAA as a BA, a BAA should no longer be required. Rather, the BA’s contractual arrangement with the subcontractor should include these same requirements.



HHS needs to understand the number and scope of business associates whose information privacy and security management practices are now to be regulated directly under HITECH, particularly in light of the expansion of the definition of business associates to include subcontractors and the OCR estimate that 1,500,000 business associates would be required to bring their subcontractors into compliance. In the NPRM, OCR does not estimate the number of covered entities and their business associates required to amend their agreements. However, in the regulatory impact statement for the Interim Final Rule on reporting of unsecured breaches of protected health information (the “Breach Notification Rule”), HHS estimated that most entities have only a few business associates. (See Breach Notification Rule, 74 Fed. Reg. 42740, 42760 (Aug. 24, 2009.)) It is common for health care providers such as a community hospital to have hundreds of business associate relationships, and large complex academic medical centers can have over 1000 business associate relationships to manage. HIMSS offers the following anecdotal information from several members, which is intended to amplify the workload impact of current practice that could be alleviated by the elimination of BAAs.

	<b># Beds</b>	<b>#BAAs</b>
Org. 1	512	356
	18	95
	n/a	20
	138	93
	25	36
	n/a	35
Org. 2	250	300
Org. 3	Large Integrated Health System	Over 1,000
Org. 4	Large Children’s Hospital	Over 350
Org. 5	Critical Access Hospital	Over 40

In addition, HIMSS is concerned that the federal government estimate of one hour of a legal professional’s time to modify these contracts, is very low and incorrectly assumes that the change can and would be made unilaterally.

Finally, mandating amendments of separate BAAs solely for the purpose of incorporating the HITECH Act privacy and security requirements will negatively impact the overall workload and increase cost within an organization. Other, important compliance efforts of covered entities and business associates will be impacted, such as, updating risk analysis and privacy and security policies on the new substantive requirements under HITECH, implementing hardware and software to prevent and monitor for unsecured breaches of protected health information, and educating the work force on the updated HITECH requirements and general privacy and security management.



Response to Office of Civil Rights (OCR) Notice of Proposed Rule Making (NPRM) on proposed modifications to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Enforcement Rules (“HIPAA Rules”) published July 14, 2010 (75 Fed. Reg. 40868).

**2. HIMSS recommends that OCR also further define the term “business associates,” with particular reference to the extent to which the conduit exception applies. HIMSS also recommends that the definition of “conduit” and “health information organization” be clarified.**

In the proposed definition of BA at NPRM §160.103, OCR would include HIOs, E-Prescribing gateways and persons providing data transmission services to a covered entity with respect to PHI and that require access on a routine basis to that PHI. OCR would exclude “mere conduits” for the transport of PHI that do not access the PHI other than on a random or infrequent basis (NPRM at 40873). OCR contrasts these conduits with entities that manage PHI through a network as having more than random access, including providing patient locator services and performing various oversight and governance functions for exchange of PHI. This definition is nebulous, and considering the regulatory consequence of the definition under the HITECH Act, needs to be clarified and explained in the final rule.

In addition, there are organizations external to the traditional frame of reference for healthcare, such as those in the banking and financial services industry that transfer health data. These organizations need to understand more fully and specifically the implications of the definition of the term “conduit” and their associated obligations are under HIPAA and HITECH. Please see the table in the attached Appendix for detailed comments/input on this topic.

Finally, HIMSS suggests OCR define “health information organization” in the final rule, and that OCR utilize the three architecture models – centralized, federated, and hybrid – that are increasingly being discussed among the HIMSS membership, and at the HIT Policy Committee and HIT Standards Committee. A clear understanding of OCR definition of HIOs and corollary connection to the architecture models’ roles as conduits will assist the healthcare community’s ability to meet the government’s requirements. HIMSS suggests OCR review the attached [HIMSS Guide to Participating in a Health Information Exchange](#), which provides an excellent overview of these architecture models.

**3. HIMSS urges OCR to provide the guidance on de-identification, limited data sets, and the minimum necessary rule at least six (6) months before the compliance date for the privacy and security modifications.**

As a result of the robust regulatory agenda under the HITECH Act, many essential elements of the HITECH Act have yet to be defined. The NPRM does not address requirements for the accounting for disclosures under HITECH §13405; the new authority of the State Attorneys General to enforce the HIPAA under HITECH §13410(e); many of the studies, reports, and guidance required by the HITECH Act; or the guidance required under HITECH §13405(b) with respect to what constitutes minimum necessary.

The healthcare community needs OCR guidance on its new obligations before compliance is expected, particularly with respect to the minimum necessary standard and the de-identification of protected health information in order to properly analyze disclosures, especially those disclosures made to business associates for healthcare operations purposes. The HITECH Act requires HHS to issue affirmative guidance on limited data sets and what constitutes the minimum amount of information necessary under HIPAA considering its own guidance on the de-identification of protected health information as well as the “information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.” Under the HITECH Act, until HHS issues this new guidance, covered entities must limit all permitted disclosures to a limited data set of the PHI or in limited circumstances, to the minimum extent necessary as determined by the disclosing covered entity. HHS should state its views on these



Response to Office of Civil Rights (OCR) Notice of Proposed Rule Making (NPRM) on proposed modifications to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Enforcement Rules (“HIPAA Rules”) published July 14, 2010 (75 Fed. Reg. 40868).

foundational issues; offer guidance to covered entities and business associates; and provide sufficient notice for compliance before sanctions are imposed.

As an example, HIMSS notes that the text discussing psychiatry notes should also include substance abuse and treatment, HIV results and treatment, and genomic data and results.

#### **4. HIMSS recommends that OCR provide for an extended period before requiring compliance under the final rule in any event.**

In the NPRM, OCR recognizes that covered entities and business associates will find it difficult to comply with the HITECH statutory provisions until the rule has been published in final form. Throughout the history of modification to the HIPAA standards and implementation specifications, a six-month period has been used to allow parties who were alert to their impending regulatory duties to implement the necessary revisions. Based on HIPAA §1175(b)(2) and the implementing provisions at 45 C.F.R. §160.104(c)(1), OCR proposes to allow covered entities and business associates a grace period for compliance no later than 180 days from the effective date of the final rule. NPRM §160.105 would provide this default 180-day compliance period for most of the privacy and security modifications. The transition provisions under NPRM §164.532(d) and (e) would deem existing BAAs compliant until the parties modified or renewed the BAA or until one year after the compliance date.

HHS has sought public comment on many interrelated issues under HITECH. Many HHS agencies have been and will continue to be involved in rule making under this groundbreaking statute. We appreciate OCR’s guidance and updated *Guidance Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable or Indecipherable to Unauthorized Individuals for Securing PHI* and the recent *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*. We understand that OCR intends to update its guidance regarding unsecured breach notification provisions in the Breach Notification Rule in the coming months. At the same time, the healthcare community is absorbing the Office of the National Coordinator’s (ONC) Final Rule on Standards, Implementation Specifications, and Certification Criteria for EHRs, the recent Center for Medicare and Medicaid Services (CMS) final rule on Medicare and Medicaid EHR Incentive Programs and Meaningful Use, and concurrently implementing ICD-10. The healthcare community also awaits a draft rule on the Accounting of Disclosures statute. However, as set forth above, the healthcare community awaits further guidance on many essential elements of HITECH.

Given the tight implementation schedule for the privacy and security provisions created by the HITECH Act, covered entities and their business associates need to use their time wisely to review HHS regulatory guidance and focus on new and revised substantive obligations and contractual modifications. As a result, HIMSS recommends that OCR exercise regulatory discretion on timing of the compliance date and further extend each of these grace periods an additional six (6) months. This need for an extended compliance period is particularly acute for subcontractors that were not previously subject to HIPAA. To the extent that OCR includes the subcontractors to business associates as business associates in the final rule, it should extend that compliance date much as was done for small health plans in the initial stages of HIPAA implementation.



**Other comments:**

HIMSS suggests the healthcare community will benefit from the government including wireless transmission in the “transmission media definition.”

In addition, HIMSS observes that the collection and transmission of immunization information to schools is an area of great importance to the community, and that the structure for accomplishing this initiative, (such as who is authorized to receive the immunization record information, and what they do with it), is still in development.

Finally, HIMSS commends OCR for requiring risk assessments in §164.308 of the NPRM. HIMSS encourages OCR to utilize the final rule to indicate that such an assessment should be repeated periodically or whenever significant changes are made to the IT environment. As we indicated in the [HIMSS comments to the Department on the Notice of Proposed Rule Making on the Medicare and Medicaid Electronic Health Record Incentive Programs](#) (lines 723-741), HIMSS members and industry colleagues are relying on the government to provide guidance on the “frequency and scope of the risk assessment.” Having a clear requirement on the frequency will provide the necessary guidance to facility-based IT professionals and security officers.

**Conclusion:**

HIMSS appreciates the opportunity to provide public comments to the Department and the Office of Civil Rights on this important Notice of Proposed Rule Making. We look forward to continued dialogue between HIMSS members and the Department, in order to achieve the benefits of the HITECH Act. If you have any additional questions please contact [Lisa Gallagher](#), Senior Director, Privacy and Security, 703.562.8816; [Edna Boone](#), Senior Director for Enterprise Information Systems, 703.562.8815; or [Thomas M. Leary](#), Senior Director, Federal Affairs, 703.562.8814.

Sincerely,

C. Martin Harris, MD, MBA, FHIMSS  
Chief Information Officer and  
Chairman, Information Technology Division  
Cleveland Clinic  
Executive Director, e-Cleveland Clinic  
HIMSS Chair

H. Stephen Lieber, CAE  
President/CEO  
HIMSS

Attachment: [HIMSS Guide to Participating in a Health Information Exchange](#), HIMSS Healthcare Information Exchange Guide Work Group White Paper, November 2009