

**COMMENTS OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)**

**To the Notice of Proposed Rulemaking: Modifications to the HIPAA Privacy,
Security, and Enforcement Rules Under the Health Information Technology
for Economic and Clinical Health Act
(Published July 14, 2010 at 75 Fed. Reg. 40868)**

**Submitted to the Department of Health and Human Services (HHS)
September 13, 2010**

On behalf of the members of the Software & Information Industry Association ("SIIA"), we appreciate this opportunity to comment on the above referenced Notice of Proposed Rulemaking. As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet.¹ SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies. SIIA welcomes this opportunity to submit comments to the Department of Health and Human Services ("HHS") regarding its proposed rule to implement the requirements of the Health Information Technology for Economic and Clinical Health ("HITECH") Act.²

Our comments focus on several practical and technological challenges posed by the upcoming expansion of HHS's jurisdiction under the Health Insurance Portability and Accountability Act ("HIPAA") to business associates and subcontractors. The HITECH Act provides that most HIPAA privacy and security requirements will apply directly to business associates, replacing the previous regime of contract-based liability. In addition, HHS has proposed amending the regulatory definition of "business associate" to include subcontractors that create, receive, maintain or transmit protected health information ("PHI") on behalf of another business associate.

The HITECH Act's new requirements for business associates, in combination with HHS's proposal regarding subcontractors, will significantly broaden the reach of HIPAA to capture thousands of companies that offer information products and services. On behalf of SIIA's members, SIIA is concerned that the application of current HIPAA regulations to this new category of entities would have significant, unintended, and adverse consequences. We are particularly troubled by the prospect that software and information products companies may

¹ Our website can be found at: www.siiia.net

² 75 Fed. Reg. 40868 (July 14, 2010).

become subject to HIPAA merely because they receive data that originated in PHI files, even if the data received is demographic rather than health-related. We therefore encourage HHS to consider carefully how best to apply its HIPAA rules and enforcement strategies to this new regulatory arena.

I. Challenges of Expanding HIPAA to the Information Sector

SIIA recognizes that the current definition of a “business associate” would largely be retained if HHS adopts the proposed rule. As a practical matter, however, the shift from contract-based liability to direct enforcement liability is a significant change for industry. Many information products companies do not focus on the health care sector, are not routinely subject to HHS jurisdiction, and have not received previous client requests to enter into business associate agreements. Other companies would be newly subject to HIPAA as subcontractors to business associates. These categories potentially encompass thousands of information products companies that, while subject to other data security and privacy regimes, are novices in HIPAA compliance.

To illustrate the challenges of expanding current HIPAA regulations to cover information products companies, consider the example of applying HIPAA to search products. Our member companies offer a wide variety of products that could be used to seek information about individuals using open-ended search queries or other types of search functions. For example, numerous companies provide free Internet search engines or tools to search their own websites. When these functions are provided at no cost to the user, the product developer generally has no contractual relationship with, or means to identify, the end user. Nevertheless, a covered entity or business associate could, at any time, use PHI to compose a search query and submit it to this type of search function. For example, a hospital fundraiser might use an online “white pages” locator to search for a former donor and patient who appears to have moved. The search engine would have no control over what data the fundraiser uses in this type of search and whether it includes health information. Indeed, there would be no way for the search engine to distinguish between a search query that involves patient PHI and one that, for example, comes from a person searching for health information for himself. Because search engines routinely retain records of past queries in order to improve search performance, the search provider may unwittingly receive and retain PHI.

Covered entities or business associates might also pay a fee to access more sophisticated information products containing individually identifiable data. For example, such products could allow the same fundraiser to search by an individual’s name or current contact information in order to locate a donor’s place of business, research her financial circumstances, or obtain demographic information to determine what type of appeal is most likely to be successful. The fundraiser would likely draw on the covered entity’s own records about the individual in order to compose the search query. Even if no health-related data is transmitted in the search query, the information product may keep a record of the search that is associated with the client as a business service, and the client’s identity may reveal a health care link. Under HHS’s current approach, HIPAA protections may attach to and follow any PHI that is transmitted through such a search query, even if it is demographic information rather than details of an individual’s health care, condition, or payment.

As SIIA has previously noted in its comments to HHS, it is important to again highlight that companies handling individually-identifiable information are subject to data protection mandates other than HIPAA. The Federal Trade Commission (“FTC”), through its enforcement actions, has made clear its position that failure to provide reasonable and appropriate security for sensitive consumer data is an unfair act or practice that violates Section 5 of the FTC Act. In addition, nearly all states have laws requiring notification of individuals affected by a data security breach. Companies may also fall within data security regimes that apply to specific types of information. For example, many information products companies are covered by the Gramm-Leach-Bliley Act, which imposes privacy and security rules for the financial industry. Thus, SIIA expects that companies are providing adequate protection for any individually-identifiable information they handle, even if these companies are outside the scope of HIPAA.

The challenges of expanding HIPAA to the software and information products sector are not limited to the search engine examples presented above. Countless other products and companies are also likely to be impacted by the new scope of HIPAA, simply through their routine business interactions with entities that collect or maintain PHI. Below, we discuss several specific aspects of the proposed HIPAA expansion that raise concerns for the software and information industry.

II. Specific Concerns

1. Entities Receiving Data May Not Be on Notice That it is PHI

To date, HHS has taken the view that HIPAA protections should follow PHI when it is transmitted to another covered entity or business associate. Previously, the required business associate agreement served to place a receiving entity on notice that the transmitted data constituted PHI and therefore that HIPAA protections were due. In contrast, under the proposed regulatory changes, a company could be deemed a business associate by operation of law the instant that PHI is received, *whether or not the entity is aware that it is a business associate or that the data is PHI*. SIIA is greatly concerned that information products and software companies will be expected to comply with HIPAA even if they receive, process or maintain individually-identifiable information without any notice that they are in possession of PHI.

Where the data exchanged between companies is clearly related to health conditions, care, or payment, it may be reasonable to believe that a receiving company will be alerted from the nature of the data itself that HIPAA compliance could be a concern. However, this expectation of inherent notice evaporates when the data being exchanged is, or appears to be, a type of data that is commonly shared without heightened HIPAA protections, such as individually-identifiable contact or financial information that does not include health information. A company that has not been asked to sign a business associate agreement and receives such data will have no knowledge or notice that the data is PHI. This risk is especially acute for companies that are “downstream” from a covered entity, such as business associates’ subcontractors, and that may receive non-health data without any apparent nexus to a covered entity. It is critical for HHS to address the plight of such companies to avoid an unfair enforcement trap.

We recognize that a company that offers data products and search capabilities to a wide variety of clients, and has contractual relationships with those clients, may have warning in some cases that a specific client is a covered entity, such as if the client is a hospital and is clearly named as such. But this suspicion or expectation that a client is a covered entity does not translate to notice that individually-identifiable data transmitted in a search query is PHI. Even if a client is known to be a covered entity, it is equally likely, for example, that an information product may be used to search for data that does not relate to patients at all. For example, a covered entity might be conducting due diligence on physicians or seeking information on employees or prospective employees, or on community residents who are potential donors.

In short, the proposed new approach would place companies, in many cases, at the mercy of their business partners to request a business associate agreement. Without such an agreement, companies may unwittingly accept PHI through their normal business conduct, and thereby violate HIPAA. This prospect creates an intolerable level of uncertainty for the information products industry, and it undermines the legitimacy of the HIPAA compliance regime.

2. Individually-Identifiable Information Without Health Information is Not Recognizable as PHI

A closely related challenge is the fact that individually-identifiable information without health information is not readily recognizable as PHI. An entity that receives this type of data therefore has little opportunity to become aware that such data may have originated in a PHI file. Nevertheless, such entities may now be deemed business associates or subcontractors by operation of law, and therefore considered to be in violation of HIPAA merely because they receive individually-identifiable data.

As a result, SIIA is greatly concerned that companies may now face substantial liability for failing to apply HIPAA protections to data that is not health-related but merely originated in a PHI file. Because the requirements of HIPAA are highly specific, companies could face liability even assuming that they provide reasonable security for all data in their possession. We do not believe that this outcome is required by, or in keeping with the intent of, HIPAA. HIPAA regulations create a tailored, heightened privacy and security regime that is designed to apply to health-related data specifically. It is simply unworkable for the specialized HIPAA rules to follow non-health data indefinitely in today's information economy, in which data sets and subsets are exchanged rapidly and frequently as a necessary part of doing business. The reach of HIPAA is not, nor should it be, unlimited. Rather, HHS should recognize that individually-identifiable data that does not include health information may lack any nexus to a covered entity, and that the application and enforcement of HIPAA is not justified without such a nexus.

3. It is Not Clear What Constitutes Activity "On Behalf Of" Another Entity

SIIA is also concerned that it remains unclear when an entity is acting "on behalf of" another entity for the purpose of qualifying as a business associate under the current rule or, under the proposed rule, as a subcontractor. HIPAA regulations offer no definition of the term "on behalf of" and HHS guidance on this issue has been scant. This lack of clarity was less

troubling when companies could rely on the existence of a business associate agreement to place them on notice of their status as a business associate. However, the regulation's ambiguity becomes a pressing issue for software and information products companies, among other industries, in an era when companies may be exposed to significant penalties for alleged compliance failures even in the absence of such an agreement.

In prior guidance, HHS has sought to distinguish between an entity that accesses PHI incidentally in the course of its services and an entity that accesses PHI routinely, setting out the general principle that an entity does not become a business associate through incidental exposure to PHI, but may qualify as a business associate if it provides a service that requires routine handling of PHI.³ SIIA believes that this type of distinction provides insufficient guidance given the expected new liability exposure for business associates because, as discussed above, software and information products companies frequently may have no knowledge or notice that information received is PHI, even if they receive it routinely.

Thus, SIIA suggests that HHS should provide additional clarification regarding when a company is acting "on behalf of" another company in a manner that triggers HIPAA requirements. SIIA notes that software and information products companies generally provide services or tools that help clients to function more effectively, but do not take over executing their clients' tasks. Such companies' role in relation to their clients is akin to that of a caddy to a golf player. While a valuable and even essential service is being provided, it would never be suggested that the caddy is golfing "on behalf of" the player. As this analogy illustrates, providing a tool that facilitates another's efforts is not generally understood to be acting "on behalf of" the other. SIIA respectfully requests that HHS provide more information or examples to clarify the business associate and subcontractor definitions, in order to minimize ambiguity and help companies understand their obligations

4. Formal Business Associate Agreements Should Not Be Required for All Business Partnerships

SIIA believes that formal business associate agreements will not be suitable for all partnerships given the complexities discussed above, and SIIA suggests that the HIPAA regulations be revised to ensure that formal business associate agreements are not required in all situations. Instead, business associate agreements should be designated an "addressable" specification under the Security Rule. As HHS is aware, companies must still meet a high compliance standard for addressable specifications. Companies must first analyze whether an addressable specification is reasonable and appropriate for that entity, and then must either (1) implement the specification, or (2) document why it is not reasonable and appropriate, and adopt any reasonable and appropriate alternative measure.⁴

³ See, e.g., HHS responses to frequently-asked questions regarding courier and mail services, software vendors, janitors, plumbers, electricians, and photocopy repair technicians, available at http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/.

⁴ 45 C.F.R. § 164.306(d)(3).

To provide more guidance to companies, SIIA further requests that the regulations should recognize additional specific circumstances when HIPAA contracting requirements can be satisfied by an “other arrangement” that accomplishes the same objectives as a formal business associate agreement, even if there is no specific reference to HIPAA. Current and proposed regulations already provide for certain situations in which entities can satisfy the requirements through “other arrangements” without a formal business associate agreement.⁵ These provisions recognize that the lack of a formal business associate agreement need not prevent data sharing as long as the data remains reasonably protected. In keeping with this approach, we believe that HHS should set forth additional circumstances when such alternative arrangements are sufficient and appropriate.

SIIA’s concerns in this area arise because an entity’s status as a business associate is now a matter of law, and thus the lack of a business associate agreement with any partner may expose companies to liability. However, due to the ambiguities discussed above, there is a likelihood that business associates and their subcontractors may reach different conclusions about whether HIPAA applies to their activities. For example, a software company may determine that it qualifies as a business associate or may be required by its covered entity clients to behave as a business associate, and it may therefore seek business associate agreements with its subcontractors. Yet a subcontractor is also entitled to seek independent legal advice and may reasonably conclude that it should not be treated as a business associate, especially if it is handling individually identifiable information with no remaining nexus to health data. The risk of such reasonable differences of opinion is likely to be especially acute in the near term, before HHS has had the opportunity to clarify its views through additional guidance and enforcement precedents. In our view, it would not be appropriate to require business associates to forego contracting with a qualified partner in this type of situation, especially because there may be no comparable vendor on the market. However, it also would not be appropriate to expose a company to liability simply because a contracting partner takes a differing view of whether HIPAA applies.

Another area of concern, as discussed above, is that a company may be legitimately and reasonably unaware that it qualifies as a business associate. Such a company therefore would not be aware of any need to establish formal business associate agreements with its partners, and it likely would not refer to HIPAA requirements in its contractual arrangements.

To address these concerns, SIIA asks HHS to consider providing regulatory accommodations so that companies, in situations like those described above, will not face HIPAA liability due to a lack of a formal business associate agreement. We believe that data security and privacy can be protected without a formal business associate agreement, because the parties can include other meaningful data protection assurances in their contract. Indeed, it is typical in the information products industry to incorporate such assurances into business contracts that relate to data handling. Thus, we encourage HHS to make the security specifications related to business associate agreements addressable rather than required. We further suggest that HHS recognize additional circumstances when HIPAA contracting requirements can be satisfied by an alternative arrangement with terms that accomplish the same objectives as a formal business associate agreement, even if there is no specific reference to HIPAA.

⁵ 45 C.F.R. § 164.314(a)(ii); 75 Fed. Reg. at 40918, 40920.

5. Application of the Media and Device Security Standard

In accordance with the HITECH Act, the proposed rule would apply the requirements of the HIPAA Security Rule to business associates. SIIA is generally concerned that this will represent a significant and costly compliance challenge for software and information products companies that have not previously been operating under business associate agreements. In the case of entities that exclusively or primarily handle individually-identifiable information with no evident nexus to health data, we are not convinced that this costly burden is necessary or required by law.

In particular, we believe that companies will face a challenge in complying with the Security Rule's mandate regarding device and media controls, at 45 C.F.R. § 164.310(d). Unlike companies that focus on the health care sector, many information products companies are accustomed to accepting data from clients in a variety of ways, according to their clients' needs. For example, a database management company may routinely accept File Transfer Protocol uploads, emailed databases and spreadsheets, and DVDs or flash drives that are delivered by hand or by post, as well as other types of electronic and physical deliveries. It would be unworkable for companies that deal with such a broad range of clients and data to apply HIPAA Security Rule protections to all such data deliveries, in any electronic medium, from the moment of their arrival. As a practical matter, a company may have no warning that a DVD arriving in the mail room contains PHI or potential PHI until that DVD reaches its destination within the company and is processed. We therefore encourage HHS to consider suspending or limiting the application of the device and media controls standard to business associates, as well as other aspects of the Security Rule as appropriate.