

**COMMENTS OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)
on the Interim Final Rule with Request for Comments
Breach Notification for Unsecured Protected Health
Information
(RIN 0991-AB56))**

***Pursuant to Section 13402 of the Health Information Technology for
Economic and Clinical Health (HITECH) Act, part of the American
Recovery and Reinvestment Act of 2009***

**Submitted to the Department of Health and Human Services (HHS)
On October 23, 2009**

On behalf of the members of the Software & Information Industry Association (SIIA), we appreciate this opportunity to comment on the Interim Final Rule with a request for comments to require notification of breaches of unsecured protected health information ("Interim Final Rule"), which was issued pursuant to Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 ("Recovery Act").

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.

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

SIIA has worked with regulators at the Federal and state levels in the United States, and also with policy makers in Europe, Canada and other regions, to examine the implications and operations of breach notification requirements since California enacted the first notification law in 2002. This has included work with the relevant federal agencies implementing existing privacy and security regulations and policies (notably, the FTC's approach on unfair trade practices where companies fail to use appropriate technological means for protecting data, as well as implementation of the Safeguard's Rule under the Gramm-Leach-Bliley Act), as well as state efforts (most notably, Massachusetts) to implement security measures.

Our comments on the above referenced Interim Final Rule take into account these experiences and industry expertise in our review of the HHS Interim Final Rule.

PRELIMINARY OBSERVATIONS

First, further consideration needs to be made of the potential conflict with existing laws and regulations involving data breach and data security. SIIA was one of the first national organizations to call for a meaningful framework on breach notification, including efforts to promote on-going security practices and plans for firms. Over the course of the last several years, the need for a meaningful national framework has grown. The threats facing mainstream companies and institutions have gotten more complex and more sophisticated. Today, the threats are increasingly external to their operations, and driven by global crime and economic fraud perpetrators. Indeed, , according to one recent study, "91 percent of all compromised records in 2008 was attributed to organized criminal activity."²

At the same time, the fragmentation of laws and regulations continues to make an effective offense against these pernicious threats more difficult, to the frustration of consumers, business and enforcement authorities. As of this writing, 45 states, the District of Columbia and Puerto Rico have implemented laws that create a divergent and patchwork approach to data breach notification. To make matters even more challenging and fragmented, at *least* 9 states have enacted prescriptive security requirements (or amended their breach laws to achieve the equivalent goal),³ some of which are inconsistent with the Guidance issued by HHS.

In this regard, SIIA commends HHS for recognizing that "contrary State law will be preempted by these breach notification regulations." However, SIIA respectfully disagrees with the statement later in the Interim Final Rule commentary that "we believe that covered entities can comply with both the applicable State laws and this regulation,"

² "2009 Data Breach Investigations Report, A study conducted by the Verizon Business RISK team", p. 13. Available at: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

³ As of January 1, 2009, these states are: Arkansas, California, Maryland, Massachusetts, Nevada, Rhode Island, Oregon, Texas and Utah.

although we appreciate the hopeful outlook that “in most cases, a single notification can satisfy the notification requirements under State law and this regulation.”

It is very likely that the Interim Final Rule will lead to potential conflicts with both state breach notification requirements and with the at least 9 states which have enacted security requirements (or amended their breach notification laws to achieve the equivalent goal). The issue is not merely *multiple* compliance obligations (as suggested in the commentary), but potentially *conflicting* procedural and element obligations which range from timing and content of notification, to the standard for determining a breach, to whether the information has been secured. We believe it is inevitable that HHS will have to address this potential for conflicting compliance obligations in its Interim Final Rule.

SIIA urges that this goal of a single notice under both relevant state law and this regulation be incorporated into the Interim Final Rule to avoid any confusion, and to facilitate the objectives of the statute and avoiding consumer confusion. In our view it appears, based on review of the requirements in many state as well as the security obligations that are emerging, that HIPAA covered entities and business associates would still be obligated to comply with many of these state statutory and regulatory obligations following a breach involving health information, such as state breach notification, as well as data security, requirements.

Second, the “Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals” in appropriately incorporates into the Interim Final Rule a number of NIST Special ‘800 Series’ Publications and FIPS . SIIA raised this substantive issue in our prior comments,⁴ but HHS did not specifically address it in its analysis.⁵

To restate the issue, the Interim Final Rule Guidance *conditions a legal safe harbor* on compliance with documents and processes of the National Institute of Standards and Technologies (NIST) that were not intended to be used in this manner. We strongly urge that any reference to NIST in the Guidance be removed to the degree that it implies that the legal basis of the ‘safe harbor’ reflected in the Guidance is predicated entirely on implementation of the NIST publications and validation procedures. Instead, HHS should recognize technologies or methodologies, either alone or in combination that may achieve the ends of rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.

⁴ See, [SIIA Submits Comments to HHS on proposed “Guidance” on Technologies for Securing Health IT Data](#), May 21, 2009.

⁵ HHS does state “that any further comments regarding this guidance received in response to the interim final rule will be addressed in the first annual update to the Guidance, to be issued in April 2010.” However, this monition does not address the factual issue raised earlier, and leaves the current Interim Final Rule Guidance faulty and inconsistent with the requirement that a rulemaking address factually substantive issues.

HHS asserts in the commentary that “the guidance on securing protected health information is not mandatory; it is discretionary.” Yet, HHS also recognizes in the commentary that “many covered entities and business associates are *voluntarily* choosing to secure their protected health information in accordance with the guidance in order to avoid the possibility of having to provide breach notifications pursuant to this subpart.” HHS does not provide support for this statement. Nevertheless, HHS misses the mark in its analysis on this point and portrays a false dichotomy. A legal safe harbor is designed to encourage good practices, not merely to avoid notification, and, therefore, neither mandatory nor voluntary. As such, the Interim Final Rule Guidance does not achieve the purposes of the Safe Harbor by relying on the stated NIST documentations and processes, many of which cannot technically be adhered to in the manner asserted in the Interim Final Rule Guidance.

First, all of the work done by NIST incorporated into the Guidance was undertaken in the context of NIST’s statutory mandate, in furtherance of its responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.⁶ “FISMA provides for the development and promulgation of Federal Information Processing Standards (FIPS) ... for *Federal computer systems*,”⁷ not for non-Federal government systems. Thus, the uniform preamble to Guidance documents clearly states that “NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all *agency* operations and assets.”⁸ As such, “This guideline has been prepared for use by *Federal agencies*. It may be used by nongovernmental organizations on a *voluntary* basis...” (emphasis added) HHS, in conditioning a legal safe harbor in this manner, has ignored the statutory limitations found in FISMA and lacks the authority to alter them in any way.

Second, the reference to the NIST publications raises a separate set of concerns regarding the suggestion in the Interim Final Rule Guidance that the “encryption processes identified [in the NIST 800-series publications] have been *tested* by NIST and *judged* to meet this standard.” (emphasis added) This language is identical to that in the earlier draft Guidance, and the commentary is silent in response to the evidence submitted previously.

This statement in the Guidance remains factually incorrect. For example, the Guidance states that it recognizes only processes that “comply with” or “are consistent with” NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User*

⁶ See Sections 303(a-d) of FISMA.

⁷ Testimony of Cita M. Furlani, Director Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce, before a Joint Hearing Before the United States House of Representatives Committee on Science and Technology Subcommittee on Technology and Innovation and Subcommittee on Research and Science Education, “Agency Response to Cyberspace Policy Review”, June 16, 2009. (emphasis added)

⁸ “...but such standards and guidelines shall not apply to national security systems.”

Devices, as well as those processes that “comply with the requirements of” NIST Special Publications 800–52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800–77, Guide to IPsec VPNs; and 800–113, Guide to SSL VPNs. Without prejudice to the useful technical analysis that is provided in these Special Publications, nothing in these referenced documents has been “tested” nor been “judged” to meet a particular standard.

On the contrary, the entire “Special Publication 800-series” reports on NIST’s Information Technology Laboratory’s *research, guidance, and outreach efforts* in computer security and its collaborative activities with industry, government, and academic organizations.” The “800-series Publications” are distinct from other NIST responsibilities which “include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems.” (emphasis added) The distinction between the 800 series and other technical standards produced by NIST is also stated clearly on the NIST website, as the former were specifically established “to provide a separate identity for information technology security publications.”⁹ Further to the lack of the “800-series Publications” as a basis for conformance evaluation, NIST has carefully refrained from labeling these Special Publications as even ‘best practices.’ It is beyond the authority provided in the Recovery Act for HHS, as a condition of a legal safe harbor, to impose on the commercial sector Special Publication requirements, many of which are not even mandatory to Federal agencies.¹⁰

The Guidance also states, in Section II.B(a)(ii), that entities must comply with “valid encryption processes for data in motion .. [which] may include others which are FIPS 140-2 validated.” The reference to FIPS 140-2 is to specifically evaluated products; it is not a reference to a “technology or methodology”,¹¹ as required in the Act. In addition to this inconsistency, the reference to specific products as provided in the Interim Final Rule risks giving unfair advantage in the marketplace to the manufacturers of those products and potentially is a stifling of innovation as covered entities and business associates may implement products that are as effective or even more effective than those that have garnered FIPS 140-2 evaluation for commercial use. To reiterate our previously stated concern with inappropriate incorporation of NIST standards into the Interim Final Rule, FIPS are developed and adopted by NIST as a standard that “is

⁹ “Special Publications in the 800 series present documents of *general interest* to the computer security community. The Special Publication 800 series was established in 1990 **to provide a separate identity for information technology security publications**. This Special Publication 800 series reports on ITL’s *research, guidelines, and outreach efforts in computer security*, and its *collaborative activities* with industry, government, and academic organizations.” Found at: <http://csrc.nist.gov/publications/PubsSPs.html> on October 23, 2009. (emphasis added)

¹⁰ The implication of HHS imposing these documents on commercial implementations raises profound questions about the process that NIST has gone through in the development of Special Publications. If HHS were to require as a legal condition of the safe harbor, as provided in the Guidance, conformance to these documents, each of these documents would have to be opened up for a formal notice and comment process. None of these documents are the product of such a process.

¹¹ The Act at section 13402(h)(2).

applicable to all *Federal agencies* that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.” While “this standard is *available* to private and commercial organizations,” FIPS have never before been imposed by federal rule or regulation as a predicate to a legal obligation, liability or safe harbor on commercial implementations.

As a general matter, SIIA is deeply concerned that the Guidance gives legal benefit only to those processes that have been tested (or, of deeper concern, ‘*certified*’) in satisfaction of the Guidance. Nothing in the authority given HHS under the ARRA permits the imposition of testing or certification requirements, *even if HHS could demonstrate that such conformance were technically possible using common place evaluations – which it has not, and we would add, could not be done.* Additionally, nothing in the record establishes that such tests or certification is a necessary prerequisite to benefitting from the safe harbor established in the Guidance.

Third, we would urge the Secretary of HHS to consider creating a separate, distinct Office to handle the implementation of the HIPAA Privacy and Security rules. The complexity of this Interim Final Rule and related rules under HIPAA, now that the data breach notification obligations have dramatically expanded their scope and impact, require that an Office that is able to interact with key stakeholders in a transparent and constructive way is warranted.

This has become the model of those agencies with responsibilities under the Gramm-Leach-Bliley Act, as well as the way the FTC operates when implementing its Section 5 authorities. Without any criticism intended of the important functions of the Office of Civil Rights at HHS, the greatly expanded scope of the HIPAA Privacy and Security rules now go far beyond the framework of individual complaints and adjudications to a much broader impact on the health sector and the economy.

We strongly recommend that the Secretary establish a dedicated Office reporting directly to her with responsibilities for implementing these rules.

KEY ISSUES IN THE INTERIM FINAL RULE

SIIA offers the following comments on the Interim Final Rule and looks forward to continuing to work with HHS as it implements this complex regime.

Applicability. The Interim Final Rule indicates that it is applicable to breaches occurring on or after 30 days from the date of publication. SIIA appreciates that HHS is taking the approach of the Federal Trade Commission (FTC), which stipulated that it would use its enforcement discretion to refrain from bringing an enforcement action for

failure to provide the required notifications for breaches that are discovered before February 22, 2010. The FTC did so because “it recognizes that entities may need to develop new procedures to comply with [the FTC’s health information data breach rule].”

As the anticipated scope of the FTC’s Interim Final Rule covers less than 1% of the number of entities covered by the HHS Rule, and in light of the significant changes – particularly in technology as effected by the Guidance – it is reasonable that HHS consider extending its discretion not to enforce beyond February 22, 2010. The technical and operational implementation issues we have identified so far are very likely to cause inordinate difficulty, given the complexity of the issues and the vast number of organizations that must comply with the rule.

Definitions.

(1) There are several issues related to the definition of ‘**breach**’.

First, SIIA agrees with the conclusion of HHS that “a violation of the Security Rule does not itself constitute a potential breach.”

Second, SIIA in part agrees with the conclusion of HHS that “for an acquisition, access, use or disclosure of protected health information to constitute a breach, it must constitute a violation of the Privacy Rule.” As such, a “use or disclosure of protected health information that is incidental to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule [citation omitted] and therefore, would not qualify as a potential breach.”

However, sole reliance on the Privacy Rule may not be sufficient to determine whether a breach, as defined in the statute, has occurred. The commentary avoided defining access and acquisition. However, without distinguishing between mere access and acquisition, the Interim Final Rule could result in unnecessary and harmful over notification to consumers, a concern that is recognized in both the FTC and HHS Interim Final Rules. More specifically, unauthorized persons may have access to information if it is available to them while the term acquisition, however, suggests that the information is not only available to unauthorized persons, but in fact has been obtained by them. To the degree that the Privacy Rule does not distinguish those terms in this way, the definition will not completely conform to the underlying statute which governs.

Third, **SIIA strongly concurs with HHS that “the statutory language encompasses a harm threshold”** and with the clarification in the definition that the phrase “compromises the security or privacy of the protected health information” means “poses a significant risk of financial, reputational or other harm to the individual.”

SIIA agrees that, as an initial matter, this is a step toward alignment with State breach notification laws – but, in our view, does not “ensure” consistency nor address other aspects of the conflicts, which we have noted above.

SIIA believes there is a second and independent reason, consistent with the statutory language and intent, for the significant risk of harm threshold in the Rule: to avoid overnotification, which can result in direct and consequential harm to individuals. This policy consideration is a serious equity, as it is widely recognized by a variety of consumer and privacy protection authorities that a notification framework:

“... might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, **notices may be more common than would be useful.** As a result, **consumers may become numb** to them and fail to spot or act on those risks that truly are significant. In addition, **notices can impose costs on consumers and on businesses**, including businesses that were not responsible for the breach. [Examples given.] Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally.”¹²

Similar concerns were expressed in April 2007, by the Identity Theft Task Force, comprised of 17 federal agencies with the mission of developing a comprehensive national strategy to combat identity theft, and which reinforces a key consideration in the protection of consumers: *There may be direct and harmful unintended consequences that may be associated with broad notification that can be avoided with a significant risk of harm threshold.*

The experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and “phishing” attacks when bad actors become aware of broad notifications. In January 2006, the New York State Consumer Protection Board (CPB) advised that scam artists were trying to cash in on the national paranoia over identity theft by luring victims with a phony warning that they may already be the victims of identity theft.¹³ The FTC was compelled to caution U.S. veterans in 2006 “to be extra careful of scams following the recent data breach at the Department of Veterans’ Affairs (VA),” noting that “[i]n the past, fraudsters have used events like this to try to scam people into divulging their personal information by e-mail and over the

¹² Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft, Presented by Chairman Majoras and the Other Members of the Commission Before the Committee on Commerce, Science, and Transportation of the United States Senate (June 16, 2005), p. 10. Found at: <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>.

¹³ See “Phishing Fraudsters Prey on Identity Theft Fears,” January 13, 2006, found at: http://www.consumeraffairs.com/news04/2006/01/cpb_phishing.html.

phone.”¹⁴ This concern with detrimental harm to consumers by over broad notification also extends to posting the incidence of breaches on the HHS website.

Such scams follow a simple, but serious pattern: Users may receive emails purporting to come from their credit card company or bank, or health care provider or insurer, referencing recent news reports of “breaches”, asking them to enter their details and account numbers for the purposes of fraud protection or to reactivate their account. Often emails may even claim a fraud has been committed against the user’s account and against the backdrop of the most recent data breach, many users will assume that news is legitimate.¹⁵

Finally, the Interim Final Rule will promote overnotification unless it makes clear that there are certain categories of transfers of health information by a HIPAA-covered entity and business associate that are necessary to the subsidiary or affiliate services that an individual expects from the vendor or entity and which do not constitute a each transfer of health information giving rise to unauthorized acquisition. These transfers are inherent to the authorization given by an individual in the context of the nexus with the vendor or entity. As such, it would be unreasonable for an individual to expect to give each such transfer individual authorization. It is appropriate, therefore, for the definition of breach, if not otherwise provided by the Privacy Rule, not to include such subsidiary or affiliate transfers and the corresponding authorizations from the vendor or entity to facilitate such transfers. To state the obvious, if the consent of the individual is required each and every time such an otherwise authorized transfer occurs, this raises both impractical operational issues and potential notification triggers that would lead to over notification.

- (2) With regard to the definition of “**unsecured protected health information**”, SIIA notes our comments in the preliminary Observations regarding the concerns and inadequacies of the Interim Final Rule Guidance.

Notification to Individuals. SIIA directs its comments to several aspects of this section of the Interim Final Rule.

With regard to **timeliness**, there is concern that the commentary to the Interim Final Rule suggests that “even if it is initially unclear whether the incident constitutes a breach” the time period for breach notification begins “when the incident is “first known, not when the investigation of the incident is complete.” SIIA urges that this not be the standard. Imposing on HIPAA-covered entities or business associates an obligation to

¹⁴ “FTC Warns Veterans to Delete Unsolicited E-mails; Scams via E-mail and Telephone Often Follow Data Breaches,” (June 2, 2006), found at: <http://www.ftc.gov/opa/2006/06/fyi0632.htm>.

¹⁵ See “Will MasterCard breach breed new wave of phishing?”, 21 June 2005. Found at: <http://software.silicon.com/security/0,39024655,39131331,00.htm>.

notify *without a full factual assessment* of the situation risks both overnotification (the hazards of which are discussed above) or, worse, hair-trigger notices being sent that may not be appropriate, inaccurate, incomplete and ultimately detrimental to the individual.

With regard to **content** of the notices, SIIA supports the thrust of the HHS commentary that appears to encourage only essential, necessary information, including describing only the types of information involved. While restating the statutory language that the notice should include a “brief description of what happened”, SIIA encourages HHS to avoid interpreting this as a requirement for the notice to describe how the breach actually occurred. To do so would have serious unintentional consequences and give the bad actors a roadmap to not only know to cover their tracks in the particular breach in question (and thereby frustrate legitimate law enforcement needs), but also for future breaches.

With regard to **methods of notification**, SIIA recognizes that the statute requires a covered entity to provide breach notice in written form by first-class mail, but may also provide it by electronic mail, provided the individual has agreed to it and not withdrawn the request. SIIA urges HHS to recognize that in some cases, imposing a unilateral requirement to notify individuals by letter through first class mail may require a covered entity to collect information (such as address) that they do not otherwise collect, especially where the covered entity operates online. In our view, informing the individual that written notice may require the collection of MORE information, which the covered entity would prefer not to do, and thereby encouraging individuals to be notified by email – consistent with the existing online relationship – is not an inappropriate communication or monition by the covered entity.

With regard to avoiding multiple notices, SIIA commends HHS for coordinating with the FTC to “ensure” individuals could not receive multiple notices of the same breach if the HHS and the FTC regulations overlapped. We note, however, that this only addresses one facet of avoiding multiple notices being sent to consumers for the same breach.

As noted above, the myriad of state laws have created a fragmented patchwork that makes it very likely that the potential concerns identified in the HHS original Request for Information as well as the FTC’s notice on this point will also be made manifest. If HIPAA-covered entities and their business associates notify under the Interim Final Rule, then it is extremely likely that they could have to notify individuals in the 45 states where separate breach notifications exist, and that the requirements for the notification in those situations are neither wholly contemporaneous nor identical. Many business associates service large national accounts so a single breach could very well affect residents of all 50 states. As a specific step, HHS should recognize the potential for this duplication and conflict, and work to the greatest degree possible to have the Interim Final Rule avoid individuals receiving multiple notices regarding the same breach incident when state laws may impose duplicative, even inconsistent, requirements.

Notification to the Secretary. As required by Section 13402(e)(4) of the Recovery Act, the Interim Final Rule states that the Secretary will post on the HHS Web site a list of covered entities that submit reports of breaches involving more than 500 individuals. We note that the statute says list of *covered entities*. However, the HHS Website describes it differently: Instead, the website states: “This page will be updated with reported breaches of unsecured protected health information affecting 500 or more individuals.”¹⁶ That is not the requirement of the statute.

This is more than mere statutory interpretation. Posting information on breaches results in adverse harm to consumers. As described more fully above, bad actors prey on notices, whether in the media, mass emails or website postings, to find incidences of breaches which they then turn into phishing scams. HHS should ensure that consumers are not adversely harmed by broad (and especially overbroad) notification via postings on its website.

SIIA also strongly urges HHS to treat any and all information submitted to the Secretary pursuant to 164.08 of the Interim Final Rule as business confidential, not subject to release under FOIA, except for that absolutely essential information required (as discussed immediately above) to be posted on the website. To treat such submissions otherwise could also compromise its potential to be evidence in a criminal or civil proceeding.

Notification by a Business Associate. SIIA commends the overall approach taken by HHS in this section taken of the Interim Final Rule, consistent with the Recovery Act that a business associate is to notify a HIPAA-covered entity, which in turn is the appropriate entity to notify affected individuals. This serves to facilitate the notice coming from the entity that the individual has the relationship with. Otherwise, consumers would be receiving notices from entities they may never have heard of, or impose requirements that fundamentally disrupt the relationship between the individual and the vendor or entity.

The Interim Final Rule appropriately recognizes that it is not necessary to stipulate by Rule that notice is to be given to a senior official or privacy official, as “covered entities and business associates already have established business relationships and communication channels,” which are already required under the HIPAA Rules.

SIIA urges several concrete changes to the approach in the Interim Final Rule that are consistent with the statute and the efficacy of the Interim Final Rule.

First, proposed Section 164.410(c)(1) requires that the notice by a business associate shall include the “identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired used or disclosed during the breach.” From our industry’s experience in managing information for clients, and our experience with prior breaches, third party processors who are business associates often do not know what kind of data

¹⁶ See <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html>.

they process for their clients. Thus, it may not be possible – indeed, it may be impossible – to identify “each individual.” More often than not, the situation following a breach will involve the third party service provider consulting with the client-covered entity to determine if, in fact, there is personally identifiable information or who the affected individuals would be.

The “identification of each individual” raises another concern, one which SIIA assumes that the HHS did not intend, particularly in light of HHS’ discussion of multiple covered entities in this section of the commentary. Where a breach involves a third party service provider business associate, there is the possibility, as recognized by HHS, that multiple covered entities may be affected. As currently written, this section of the Interim Final Rule would require a third party service provider to *provide the identification of each affected individual to all such entities*. This would, of course, exacerbate an already problematic situation. A better approach, in the event of a breach involving a service provider business associate affecting potentially multiple covered entities, would be for the Interim Final Rule to stipulate that the third party service provider business associate (to the degree it is able, consistent with our analysis above, to provide such identification) should only do so to the covered entity which owns and licenses the particular breached information relative to the “identification of each individual.”