

COMMENTS OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)
To the Request for Information (RFI) on the
Guidance Specifying the Technologies and Methodologies That
Render Protected Health Information Unusable, Unreadable, or
Indecipherable to Unauthorized Individuals for Purposes of the
Breach Notification Requirements under Section 13402 of Title XIII
(Health Information Technology for Economic and Clinical Health Act)
of the American Recovery and Reinvestment Act of 2009

Submitted to the Department of Health and Human Services (HHS)
On May 21, 2009

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 has worked 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, and 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 work in this area is also on the global front, where SIIA engages policymakers in Europe, China, Canada and other regions on these complex issues.

Our comments on the above referenced Guidance takes into account these experiences and industry expertise.

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

GENERAL OBSERVATIONS

At the outset, we want to commend HHS for issuing this guidance within the 60-day window, as required by section 13402 of the American Recovery and Reinvestment Act (ARRA). SIIA urged Acting Secretary Johnson to take this step in our letter of March 12, 2009,² because the consequences of not doing so would be “extremely disruptive to consumers, health care providers and vendors” with real potential for “confusion and disruption for users, vendors and entities relying on existing products that achieve the stated aims of the Act but do not meet this particular [alternative] requirement is enormous.”

SIIA also commends HHS for determining that the guidance will apply to breaches 30 days after publication of the forthcoming interim final regulations.

We very much appreciate the compressed time frame in which the Guidance was required to be developed and understand that the approach taken may reflect a desire to “get something out the door” to avoid the worst case outcome established in the ARRA. We recognize the poorly drafted timelines in the ARRA, which mean that the Guidance will be an integral part of the interim final rule, which is required to be implemented by mid-August. As such, SIIA reserves final comments on the Guidance until HHS has issued a draft of the interim final rule for comment so that they can be read as an integrated whole. We note that HHS has not issued a draft, in contrast to the FTC.³ SIIA urges HHS to issue an updated RFI on the Guidance prior to the implementation of the interim final rule, given the complexity of this issue, its relationship to more than one rulemaking process, and the high likelihood of confusion that could result.

As our comments below indicate, it is the view of SIIA that there is much work to be done on this Guidance before it is finalized prior to the implementation of the interim final rule. The comments below recommend concrete steps to reflect the diversity of entire information management cycle that is now touched by this dramatically expanded coverage of health information under the ARRA, as well to achieve the goal of the legislation not to focus on too narrow a set of technologies and methodologies.

ENGAGE IMPLEMENTERS OF THE GUIDANCE DIRECTLY

From our experience over the years in working with other federal and state agencies, identified above, in implementation of various ‘safeguard’ or ‘security’ policies, it has

² [insert]

³ “FTC Publishes Proposed Breach Notification Rule for Electronic Health Information,” April 16, 2009, available at: <http://www.ftc.gov/opa/2009/04/healthbreach.shtm>.

been essential to engage relevant oversight offices directly, as issues arise that require iterative and on-going discussions among experts in both the public and private sector. Whether through roundtables, briefings or public forums with stakeholders and affected interests, an open engagement has proven to be a key step to ensure that any confusion is mitigated, as well enabling a robust dialogue on implementation issues. With the FTC deeply involved in the implementation of the ARRA in this area, such efforts should be jointly undertaken.⁴

To be candid, the ability to date to interact with HHS stands in stark contrast to the track record of other federal agencies (FTC, financial regulators implementing GLBA), and with states, such as Massachusetts (where the technical issues of that state's security regulations parallel the challenges of the HHS Guidelines), where the interaction has been meaningful, transparent and broad-based. To be specific, our efforts to garner even basic information to date has been met with monitions from HHS that discussions are not permitted over the telephone, and that any questions should be submitted in writing. With all due respect, this is not a sound basis for assuring that the policy is implemented effectively nor an approach that serves the interests of consumers, businesses who are implementing the policy, nor for our shared goal of protecting information and combating the pernicious effects of identity theft, fraud and misuse of information.⁵

Moreover, given the extremely short time period for implementation of this Guidance requires a more dynamic and iterative process.

RECOMMENDED CHANGES TO THE GUIDANCE

Based on our review of the current draft, taking into account the provisions of the ARRA as well as widely used and reliable technologies and methodologies, SIIA recommends the following changes to the Guidance.

Treatment of Encryption (Section II.B.a) The Guidance includes, by way of "exclusive" list, encryption as one of only two recognized technologies or methodologies. As a well recognized tool for ensuring the confidentiality (and authentication) of information, encryption can be an important tool that is part of the overall approach to secure information practices.

However, the Guidance places inordinate -- and inappropriate -- reliance on documents and processes of the National Institute of Standards and Technologies (NIST). We strongly urge that any reference to NIST in the Guidance be removed as it implies that

⁴ SIIA notes that this recommendation is consistent with the provisions of Section 13502(h) of ARRA, which specifies that the guidance should be developed "after consultation with stakeholders."

⁵ We note that, as of this writing, we have still not received a written response to our letter of March 12, 2009.

the legal basis of the ‘safe harbor’ reflected in the Guidance is predicated entirely on implementation of the NIST publications and validation procedures.

First, all of the work done by NIST cited in the Guidance was undertaken in the context of NIST’s statutory mandate, which is in furtherance of its responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. Thus, “NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all *agency* operations and assets.”⁶ As such, “This guideline has been prepared for use by *Federal agencies*. It may be used by nongovernmental organizations on a voluntary basis...” We are aware of no other federal rule or regulation that has attempted, directly or indirectly, to impose NIST requirements on the commercial sector as predicate to a legal obligation, liability or safe harbor. It is inappropriate, and outside of HHS’ authority, to change the requirements of FISMA or alter them in any way.

Second, the reference to the NIST publications raises a separate set of concerns regarding the suggestion in the Guidance that the “encryption processes identified [in the NIST publications] have been *tested* by NIST and *judged* to meet this standard.” (emphasis added) SIIA is deeply concerned that the Guidance implies, or may lead to, the assumption that that only those processes that have been tested (or, worse, ‘*certified*’) satisfy the Guidance. Nothing in the authority given HHS under the ARRA permits the imposition of testing or certification requirements. Moreover, nothing in the record establishes that such tests or certification is a necessary prerequisite to benefitting from the Guidance safe harbor.

Moreover, the Guidance is factually incorrect. Several of the documents cited reflect neither results of “tests” nor a “judgment” about a particular standard, as asserted in the Guidance. For example, the Guidance states that it recognizes processes that “are consistent with” NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User 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 and the well recognized role of NIST as a facilitator with industry in this important area, *nothing in these 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,” and is 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) In

⁶ “...but such standards and guidelines shall not apply to national security systems.”

fact, NIST has carefully refrained from labeling these Special Publications as even ‘best practices’ and it is beyond the legal authority of HHS to impose on the commercial sector Special Publication requirements that are not even mandatory to federal agencies.⁷

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.” SIIA again states its concern that HHS is exceeding its legal authority to impose testing and certification requirements on commercial implementations. Moreover, the reference to FIPS 140-2 is not a focus on a “technology or methodology”, but instead a reference to specific products, which is not found in the ARRA. And, as pointed out above relative to the Special Publications, FIPS are developed and adopted by NIST as a standard that “is 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 been imposed by federal rule or regulation as a predicate to a legal obligation, liability or safe harbor on commercial implementations.

Based on this analysis, and the serious problems that the Guidance would create if it is to reference encryption as currently drafted, SIIA recommends that the Guidance, consistent with the legal requirements of the ARRA, merely state “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and such confidential process or key that might enable decryption has not been breached.”

Other methods to render data unusable, unreadable, or indecipherable.

The Guidance posits a stark approach whereby only use of encryption (and, more specifically, only specified implementations of encryption designed for government agencies) or media destruction satisfy the ARRA directive to render data unusable, unreadable, or indecipherable.

As an initial matter, we want to focus on the Guidance’s treatment of de-identification. We very much appreciate and concur with the conclusion of HHS that “once PHI has been de-identified in accordance with the HIPAA Privacy Rule [citing 45 CFR 164.514(b)], it is no longer PHI (protected health information), and therefore no longer subject to the HIPAA Privacy and Security Rules.” That statement is consistent, in our view, with the operation of the Rules.

⁷ 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 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.

However, the standard in the ARRA with respect to the *purposes of the breach notification requirements under Section 13402 of Title XIII* is different in both context and specificity from that related to de-identification, which pre-exists in HIPAA. The standard in the ARRA was developed in the context of whether a “breach of security” had occurred (thus, warranting breach notification), and not as a threshold for whether the requirements of the Privacy and Security Rule have been met. Thus, the question of whether data has been rendered unusable, unreadable, or indecipherable does not depend on evaluating whether complete ‘de-identification’ has occurred, as that latter standard goes way beyond what is typically meant by unusable, unreadable, or indecipherable PHI data.

The contrast is stark when the elements of the de-identification rule are considered vis-à-vis the requirements of the ARRA. With de-identification, the Privacy and Security Rule requires, in part, that all the elements be ‘removed.’⁸ Moreover, the other method of ‘de-identification’ is an approach “for rendering information not individually identifiable.”⁹ This, too, is a different standard that provided for in the ARRA.

In our view, it is therefore appropriate for the Guidance to recognize specific methodologies (and not merely repeat the current requirements of the Privacy and Security Rule) such as redaction, truncation and obfuscation since these tools, when applied in a manner that renders data unusable, unreadable, or indecipherable is appropriate and consistent with the interim final rule. This approach will meet the legal threshold for not warranting breach notification in the event of “the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual.”¹⁰

There is a legal and policy basis for this distinction, in our view. A fundamental thrust of a data breach notification framework, articulated by the FTC in its proposed interim final rule, is that “the entity that has experienced the breach is in the best position to determine whether unauthorized acquisition has taken place.”¹¹ This creates a presumption that unauthorized persons have acquired information if they have access to it, thus creating an obligation to provide notification which “can be rebutted with reliable evidence showing that the information was not or could not reasonably have been acquired.”¹²

We would also note that there is a policy judgment about avoiding overnotification which is implicit in this judgment, as well, based on the fact that consumers, in fact, are being preyed upon by bad actors following massive notifications. In January 2006, the New York State Consumer Protection Board (CPB) advised that scam artists were trying to

⁸ 45 CFR 164.514(b)(2).

⁹ 45 CFR 164.514(b)(1).

¹⁰ Section 13407(f)(1) of the ARRA.

¹¹ FTC Proposed Interim Rule, at p. 9.

¹² Ibid.

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 Even in the well publicized breach involving the U.S. Department of Veterans Affairs – where no incident of identity theft was determined to be attributable to the breach -- the U.S. Federal Trade Commission was compelled to caution U.S. veterans in 2006 because of the *harm from subsequent criminal activity* “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 phone.”¹⁴

Thus, this is the area between ‘de-identification’ (which anticipates *removal* of the information) and the thresholds established by the ARRA: where PHI data will have been rendered usable, unreadable or indecipherable, there is no obligation (nor need) to notify.

HHS determining the Guidance is an “exhaustive” list. HHS states that “that the technologies and methodologies referenced ... in Section B are intended to be exhaustive and not merely illustrative.” (p. 13) HHS does not explain the statutory basis for determining that technologies and methodologies included in the Guidance are “exhaustive.” On the contrary, section 13402(h) of ARRA envisions at least annual updates of the Guidance, which means it will be far from “exhaustive.” Moreover, SIIA strongly recommends that HHS include a catch all for “any other technology that renders data unreadable, unusable or indecipherable” that may not be specifically referenced in the Guidance.

HHS inquiry regarding “PHI in limited data set.” HHS asks whether PHI in limited data set form should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification, and thus, included in this guidance. It is the view of SIIA that such data should be treated as unusable, unreadable or indecipherable for purposes of breach notification. As HHS correctly points out, the existing HIPAA Privacy Rule already recognizes the distinction, and including the creation of a limited data set in the Guidance (or in the interim final rule) would better align the federal approach on health care information with state breach notification laws (which are increasingly complex) and focus on direct identifiers; and that there are real administrative and legal difficulties that covered entities (and PHR related entities, as defined by the FTC) face in notifying individuals of a breach of a limited data set in light of the limited contact information and requirements in data use agreements.¹⁵

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

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 SIIA notes that the question posed by HHS on limited data sets further supports our recommendation for including redaction, truncation and obfuscation, since state breach notification laws are generally predicated on a *risk analysis* approach to unauthorized acquisition.

The Guidance underestimates the myriad of laws that impact compliance with the Guidance, including State laws and regulations on data security. The draft Guidance notes that “covered entities and business associates [and SIIA would note PHR-related entities as well, as proposed by the FTC proposed Rule] still must comply with all other federal and state statutory and regulatory obligations that may apply following a breach of PHI, such as state breach notification requirements, if applicable.” (pg. 10) In the view of SIIA, the Guidance underestimates the potential conflicts, which go well beyond breach notification requirements. In a disturbing trend, at least 9 states have enacted security requirements (or amended their breach laws to achieve the equivalent goal).¹⁶ Our preliminary review of the Guidance and the requirements of at least some of state security regulations suggest, contrary to the statement in the Guidance, that the issue is not multiple compliance obligations, but *conflicting* obligations with regard to securing data or making it unreadable, unusable or indecipherable. We believe it is inevitable that HHS will have to address this potential for conflicting compliance obligations either in the Guidance or in its proposed Interim Final Rule.

For further information on this matter, please contact :

Mark Bohannon

General Counsel & SVP Public Policy

Software & Information Industry Association (SIIA)

1090 Vermont Avenue, NW 6th Floor Washington, DC 20005

Direct Line: 202-789-4471

Main Switchboard: 202-289-7442

Fax: 202-289-7097

Email Mbohannon@siia.net

¹⁶ As of January 1, 2009, these states are: Arkansas, California, Maryland, Massachusetts, Nevada, Rhode Island, Oregon, Texas and Utah.