



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

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

Dear Secretary Sebelius:

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 interim final rule, entitled, *the Interim Final Rule on Breach Notification for Unsecured Protected Health Information* that was posted on the Department's website and the Federal Register on August 24, 2009.

HIMSS is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of healthcare. HIMSS represents more than 24,000 individual, 380 corporate members, and 46 chapters nationwide. HIMSS seeks to shape healthcare public policy and industry practices through its educational, professional development, and government relations initiatives designed to promote information and management systems' contribution to quality patient care.

As in past responses to HHS, HIMSS has leveraged the subject matter expertise of our members to ensure that our response reflects the broadest level of industry experience. For the response on the guidance document, our Privacy and Security Steering Committee played an important role in encouraging comments from colleagues across HIMSS communities. These cross-professional viewpoints ensure that HIMSS fulfills its requirement to offer a coordinated voice to the national discussion on these important healthcare issues.

As you know, the American Recovery and Reinvestment Act of 2009 (ARRA) requires HHS to issue interim final regulations within 180 days to require Covered Entities and Business Associates, as defined by the Healthcare Insurance Portability and Accountability Act (HIPAA) to provide notification in the case of a breach of protected health information. HIMSS appreciates the Department's interest in seeking public comment on this issue, and offers the following observations.



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

Summary Comments on IFR

Definitions (§164.402; IFR 42767)

- 1) **Significant Harm Standard** - Section 13400(1)(A) of the Act defines the term “breach” to mean “the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”

At IFR 42744, HHS has interpreted this definition to mean that “the covered entity must determine whether the violation compromises the security or privacy of the protected health information.” Also, HHS has stated that the definition encompasses a **significant harm threshold** and has clarified, in paragraph (1) of the definition (§164.404; IFR 42767), that the phrase “compromises the security or privacy of the health information” means “poses a significant risk of financial, reputational, or other harm to the individual.”

HHS further stated that this interpretation “ensures better consistency and alignment with State breach notification laws, as well as existing obligations on Federal agencies (some of which also must comply with these rules as HIPAA covered entities) pursuant to OMB Memorandum M–07–16 to have in place breach notification policies for personally identifiable information that take into account the likely risk of harm caused by a breach in determining whether breach notification is required. Thus, to determine if an impermissible use or disclosure of protected health information constitutes a breach, covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In performing the risk assessment, covered entities and business associates may need to consider a number or combination of factors, some of which are described below (stet).”

HIMSS Comments on Significant Harm Standard:

HIMSS appreciates the opportunity to comment on the Significant Harm standard. The majority of HIMSS members providing input support the significant risk of harm standard for determination of notification by the breaching entity, noting the need for practicality, good judgment and reasonableness in the rule. Without a clearly articulated and risk-based harm standard, our members foresee an increased burden on providers and consumers alike.

As drafted, the significant risk of harm standard requires the covered entity to weigh the possible risk to consumers of “financial, reputational or other harm.” The inclusion of the “other harm” category means that the types of risks to be evaluated are quite broad. HIMSS believes that it is appropriate to maintain this standard,



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

which is similar to the risk assessments required under the HIPAA Security Rule, the standards set forth in many state notification statutes and those applicable to many Federal agencies.

To ensure its practical use, HIMSS encourages HHS to provide additional guidance on this type of risk assessment required by the Rule to make a notification determination, in order to ensure widespread standardization of the process. Such guidance could include real world examples and bright line tests. As part of the guidance, HHS should consider including a list of factors that should be considered when assessing risk, the "weight" of each factor, and examples of cases in which significant risk of harm should be determined to exist.

The HHS guidance would serve to limit unnecessary, costly, and potentially erroneous interpretations of the regulatory intent. It should be clear to all parties involved what would generally constitute a breach and when notification is required. Any mitigating circumstances can of course be stated by the notifying entity in the letter of notification as they see fit, however there should be no doubt to whether such notification is required.

The federal government has initiated a process that encourages and incentivizes meaningful use of health IT and health information exchange. HIMSS supports public policy on notification that advances a practical approach to notification. Unrealistic notification standards that are onerous to implement could serve as a deterrent to the adoption of health IT solutions, including electronic health records, and associated meaningful use that is intended to improve access to quality and cost effective healthcare delivery.

HIMSS notes that at this time there is little evidence that the risk to the patient due to a breach outweighs the overall benefits of legitimate health information exchange. To "impair the process" in a way so as to deter adoption could significantly impede the nationwide initiative to increase adoption and establish widespread meaningful use of health IT solutions.

Similarly, HIMSS is concerned that a notification process that is not based on a reasonable risk assessment process could lead to increases in volume of notifications that could become unmanageable for provider organizations if all breaches require notification. HIMSS supports the approach to allow individual organizations to determine localized risk assessment processes that will set facility-based notification thresholds.

An overly broad notification process also could have a significant adverse impact on the healthcare consumer. Excessive notification could result in patient "notification fatigue" if they are notified of many breaches that would not reasonably be viewed as presenting a significant risk of harm. We believe that one important goal of the



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

notification requirement is motivating consumers to take appropriate action if there is a significant risk of identity theft. Despite mitigation efforts by covered entities, prompt consumer action after a significant breach may be critical to reduce the risk of financial loss and the complex consequences of medical identity theft. In this age of “information overload” consumers may be less likely to check their credit reports and medical records if these notices are provided in situations that do not present a significant risk of harm.

In addition, HIMSS is aware that many states have existing significant risk of harm provisions that include notification. For the sake of standardization, it is essential for the federal government to be consistent with state-level regulations and perhaps consider promulgating uniform regulations that cross state boundaries to govern protection of electronic patient health information in exchange scenarios.

Finally, HIMSS is aware of the letter from several Members of Congress regarding “Congressional intent” with regard to the statutory treatment of the term “breach” as well as the interpretation that the statutory language does not “imply a harm standard.”¹

However, we also recognize that as a legal matter, HHS has the flexibility to interpret, clarify, define, make common sense, and provide explanatory guidance in the rule. Therefore, we view that HHS’s inclusion of the harm standard is reasonably within their purview.

2) Breach Exclusions (§164.402 (2))–

a) “Good Faith Exception” (§164.402 (2)(ii); IFR 42767) – the “good faith exception” applies if there is not further “acquired, accessed, used or disclosed by such employee or agent.”

HIMSS Comments on Good Faith Exceptions:

HIMSS appreciates the opportunity to comment on this area of the Interim Final Rule. We note that there are several anticipated scenarios that could render this provision ineffective. First, the subsequent use or disclosure of such PHI may be completely legal and appropriate. Yet, as written, such use or disclosure would appear to undo the good faith exception.

Second, it appears that while the subsequent use or disclosure may be in good faith, such use or disclosure could *later* undo the good faith exception. It would be one

¹ [October 1, 2009 letter to Secretary Kathleen Sebelius](#) from the following Members of Congress: Henry Waxman, Charles Rangel, John Dingell, Frank Pallone Jr, Pete Stark, and Joe Barton.



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

thing to say a subsequent use or disclosure that is not in good faith is not protected, but as written, the language appears to say that the original good faith acquisition can become a breach when an action is taken at some later time.

3) Unsecured Protected Health Information (IFR 42741) and (§164.402; IFR 42768)

HIMSS Comment Summary on Unsecured Protected Health Information:

HIMSS appreciates the opportunity to comment on the issue of unsecured protected health information. HIMSS recognizes that many health care entities have deployed technologies/applications in the past that now may not or do not meet the standard for encryption as specified in the Rule. That is, the vendor product uses an encryption technology or methodology that does not meet the National Institutes of Standards and Technology (NIST) or Federal Information Processing Standards (FIPS) guides. This has caused concern as these organizations now face having to deal with either a vendor who needs to bring its solution up-to-speed or the ominous outcome of having to replace a current solution. The IFR does not provide guidance regarding existing technologies that do employ some form of encryption but do not meet the new rule requirements.

HIMSS appreciates the fact that “black and white” standards are necessary, and that continued waivers could be detrimental to security policy. However, several factors, including the current economic downswing and the age of legacy systems presents a real challenge for many healthcare providers. HIMSS suggests that HHS consider providing guidance and/or standards that support a progression, timeline and/or pathway from legacy systems to systems/products that meet updated requirements and synchronize the encryption requirements with the 2011, 2013, 2015 meaningful use benchmarks.

In addition, HIMSS notes that with the “safe harbor” for encryption technologies meeting HHS standards embedded in the definition of Unsecured PHI, healthcare organizations will necessarily require that some mechanism for identifying encryption technologies currently meeting the standards (e.g., certification process, centralized list, etc.) should be promulgated by HHS or NIST, so that the requirements for attaining safe harbor are clear for Covered Entities (CEs) and Business Associates (BAs).

Notification (§164.404; IFR 42768) –

- 1) Discovery of a Breach (IFR 42749) (§164.402(2); IFR 42768) – §13400(2) of the Act states that a breach is treated as discovered on the first day it is known or "should reasonably have been known to such entity."



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

In the IFR, HHS has taken the above reasonability test and interpreted it to include a diligence standard: “We have also modified the statutory language slightly to better conform to existing language in the HIPAA Enforcement Rule by incorporating the term “by exercising reasonable diligence.” The term “reasonable diligence” means the “business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.” We have made these clarifications for consistency and uniformity across the regulations.”

At IFR 42749, "reasonable diligence" is a defined term under the Enforcement Rule (45 CFR §160.410), meaning the exercise of "business care and prudence," a term that is not further defined elsewhere.

HIMSS Comments on Discovery of Breach:

HIMSS appreciates the opportunity to comment on this area of the Interim Final Rule. HIMSS is concerned that little or no precedent regarding published enforcement decisions exist to guide the CEs and BAs. We recommend that HHS consider providing guidance on the expectations for exercising reasonable diligence considering the state of the industry and technology.

Because CEs and BAs could be liable for failing to provide notice of a breach when the CE or BA did not know – but by exercising reasonable diligence would have known – of a breach, it is essential for such entities to implement reasonable technical and procedural systems for discovery of breaches. The HIPAA Security Standards require CEs (and under the Act, also BAs) to “implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” (45 C.F.R. §164.312(b))

Given how new the technology is in health IT, it is not altogether clear what kind and frequency of monitoring would meet the standard of “reasonable diligence.” HHS should consider departing from the rather demanding “imputed knowledge” standard (business care and prudence) in favor of a more flexible standard, especially with regard to emerging technologies like EHRs that simply may not have the functionality to identify breaches without almost daily audits and monitoring of systems.

Finally, HIMSS suggests that HHS consider providing additional guidance on breach detection in order to meet the public expectation of protection under the statute.

- 2) Breaches by BAs (§164.410, IFR 42769) – The IFR (§164.410 (a)(1)) that “a business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.”



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

HIMSS Comments on Breaches by Business Associates:

HIMSS appreciates the opportunity to comment on this important topic. We offer two scenarios for consideration. There are two assumptions about the BA doing so that are not always true: First, that the CE still exists and, second, that the demise of the CE led to the destruction of the Personal Health Information (PHI) held by the BA. The HIPAA Privacy Rule (§164.504e)(2)(ii)(I)) discusses the BA's contractual obligation when the contract ends regarding management of PHI obtained from the CE - it allows for the possibility that the PHI will be held (and protected) by the BA.

However, under the proposed rule, there does not seem to be any means provided to support notice of breach discovered by a (former) BA when the CE no longer exists. It is also not clear what a BA must do if it was no longer under contract with the CE, but still holds PHI obtained from the CE at the time of the breach.

Another variation on this issue is when a CE is sold/merged into another CE. The CE might still be said to exist, but if the PHI was held by the BA after the contract ended, the BA may not be aware of new CE's role with regard to the PHI and may not know how/where to report a breach. As more CEs share data with BA-type HIEs and commercial data management groups (e.g., ASP model EHR companies and/or online backup services), this situation of *orphaned PHI* will occur more frequently than it does now. It would be helpful for HHS to provide a clear and practical way for notice to be given in such circumstances, perhaps incorporating similar requirements already provided for a CE that cannot locate a patient for breach notification, i.e., regional newspapers, last registered agent with the entity's Secretary of State office, etc.

HIMSS members are also concerned with the timeliness of notification with regard to BAs at §164.410, IFR 42769. There was concern regarding the notice of unsecured PHI breach required from BAs to CEs relating to the timeliness of BA notice to their covered entity principals. Under §164.410(b), BAs must notify covered entities of unsecured PHI breach without unreasonable delay but no later than 60 days from the date the BA discovers the breach. However, if the BA is considered an agent of the CE under federal common law of agency, then the BA's discovery triggers the CE's 60-day deadline for reporting the breach to individuals. §164.404(a)(2). HIMSS suggests the Department consider whether the CE should get a reprieve in the event the BA failed to timely report the breach to the CE or even if the BA did not delay unreasonably, and that the trigger date should be the date of CE discovery unless reasonable diligence on the part of the CE could have avoided the lack of notice. . HIMSS members' experiences suggest that federal common law of agency turns on control. These types of relationships imputing discovery of breach to the CE should be rare and limited to these BAs over which CEs exercised dominion and control.



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

Finally, HIMSS is concerned about the content of the notification to individuals (§164.404) and whether it is appropriate to require the CE to report any sanctions imposed on its workforce involved in the breach. HIMSS suggests the department address the potential that this punitive framework could discourage internal reporting of incidents and impede the necessity of looking at security breaches as a systemic problem with root causes.

- 3) Breaches within Health Information Exchange organizations (HIEs) – The Act (§13408) modifies HIPAA to define HIEs as BAs when they routinely require access to PHI belonging to the CE. However, the IFR is silent on breach notification with regard to HIEs, unless one assumes that they fall under the requirements of a BA in this regard – a reasonable assumption.

HIMSS Comments on Breaches within Health Information Exchanges:

HIMSS appreciates the opportunity to comment on this important matter as many of our members expressed strong concern with the lack of separate discussion regarding breaches within a health information exchange (HIE). HIMSS recommends that HHS promulgate guidance that includes approaches for addressing HIE-related scenarios that make breach detection difficult such as identifying the responsible party; and therefore the party responsible for breach notification.

An example of a relevant scenario is as follows

There could be a potential disconnect between discovery of breach, knowledge of a breach, and responsibility for breach notification. There may be many CEs that participate in one single HIE. Many situations will involve data stored on several different servers downloaded to platforms located elsewhere in cyberspace. The actual location or responsibility for a breach in such situations is not clear. The bill would seem to assign responsibility to every party that has knowledge of a breach, even if that party was not responsible for the breach. This may create obligations on numerous CEs, create conflicts, and create confusion for patients and CEs alike. Redundant notifications or notifications where there is little possibility of further harm would only confuse and worry patients, and create needless burdens for those in health care operations. So, the clarifying question to be answered is - if one CE discovers a breach but was not responsible for the breach, does that CE have a notification obligation? This is particularly of concern when the breach occurs in an HIE because often the source or cause of the breach is unclear. At the same time, there is almost always a single entity responsible for governance of the HIE, management of the HIE applications, etc. Perhaps this is where the responsibility for determining should reside.



**Healthcare Information and Management Systems Society (HIMSS)
Public Comment on**

Public Docket Number RIN 0991–AB56, Interim Final Rule on Breach Notification

The Rule should also include a process for notifying individuals if an HIE entity is no longer available or operational.

Finally, the concept of minimum necessary also makes it difficult to determine if there was a breach and where the breach originated. (We recognize that guidance on minimum necessary is forthcoming from HHS and hope that it addresses HIEs directly).

Meaningful Use – One significant issue of concern is that of “meaningful use” and how the breach notification rules in the IFR would interplay with the eligibility of providers for the incentive payments under ARRA, as that definition evolves, becomes refined, and is adopted by the CMS rule. We note that under current informal interpretations, healthcare providers would not be eligible for incentive payments if there is a HIPAA/ARRA violation and the CE has not “repaired or remediated the defect.” HHS should solicit and consider public comment on what should be considered adequate remediation under a substantive rule. The issue revolves not just around the remedy for the patient, but also about identifying the root cause of problem and focusing the remediation on addressing the results of the root cause analysis.

Conclusion:

The American Recovery and Reinvestment Act creates many challenges and opportunities for the federal government and the healthcare community. We appreciate your effort to engage healthcare stakeholders in reviewing the guidance document, and look forward to future dialogue with HHS on this important issue. Our staff points of contact are [Mr. Thomas M. Leary](#), Sr. Director for Federal Affairs and [Ms. Lisa Gallagher](#), Sr. Director for Privacy and Security.

Sincerely,

A handwritten signature in black ink that reads "Barry Chaiken".

Barry P. Chaiken, MD, FHIMSS
Chair, HIMSS Board of Directors
CMO, DocsNetwork, Ltd.

A handwritten signature in black ink that reads "Steve Lieber".

H. Stephen Lieber, CAE
President/CEO
HIMSS