Supporting Statement for the HITECH Act Breach Notification

A. Justification

1. Circumstances Making the Collection of Information Necessary

Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub.L. 111–5) requires the Office for Civil Rights (OCR) to collect information regarding breaches discovered by covered entities and their business associates under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164). ARRA was enacted on February 17, 2009. The HITECH Act (the Act) at § 13402 requires the Department of Health and Human Services (HHS) to issue interim final regulations within 180 days of enactment to require HIPAA covered entities and their business associates to provide notification in the case of a breach of unsecured protected health information. Based on the statutory provisions, §§ 164.404 and 164.408 of the interim final rule require HIPAA covered entities to notify affected individuals and the Secretary of a breach of unsecured protected health information. Additionally, if the breach involves 500 or more residents of a State or jurisdiction, the covered entity must also notify the media pursuant to § 164.406. Business associates must notify the covered entity of any breaches that occur subject to § 164.410 of the final rule, and finally, under § 164.530(j)(1)(iv), covered entities must maintain appropriate documentation to comply with their burden of proof under § 164.414.

2. Purpose and Use of Information Collection

The final rule implements statutory provisions that require covered entities and business associates to provide appropriate notifications following the discovery of a breach of unsecured protected health information. Pursuant to § 164.404 of the final rule, covered entities must provide notification of a breach to affected individuals to alert them that their protected health information has been compromised and to encourage them to take the necessary steps to prevent any resulting harm. Covered entities must provide individuals with written notice or, if the individual agrees, with electronic notice. Substitute notice must be provided if the covered entity has insufficient or out-of-date contact information for any of the affected individuals. If there are less than 10 individuals for whom there is insufficient contact information, substitute notice can be provided by an alternative form of written notice, telephone, or other means. If there are 10 or more individuals for whom there is insufficient contact information, the substitute notice must be in the form of a posting on the covered entity's web site or notice in major print or broadcast media in the geographic areas where the affected individuals likely reside.

Under § 164.406 of the final rule, in situations in which a breach affects 500 or more individuals in a particular State or jurisdiction, the covered entity must notify prominent media outlets serving that State or jurisdiction. The purpose of this media notification, which must be provided in addition to individual notification, is not to alert affected individuals of the breach. The purpose of media notification is to alert the public that a covered entity has experienced a breach.

Section 164.408 of the final rule also requires covered entities to notify the Secretary of breaches. Covered entities must notify the Secretary without unreasonable delay and not later than 60 days for breaches that affect more than 500 individuals. For breaches that affect 500 or less individuals, covered entities must provide notice to the Secretary annually. This is the only portion of this new information collection in which OCR will receive information from covered entities. OCR will maintain the information received to ensure compliance with the provisions of the interim final regulations, as well as with the HIPAA Privacy Rule. Information collected regarding breaches of unsecured protected health information involving more than 500 individuals will be posted on an HHS web site pursuant to the requirements of the Act. Additionally, information collected will be used to create a report to Congress required annually by § 13402(i) of the Act.

Additionally, if a business associate discovers a breach, § 164.410 of the final rule requires the business associate to notify the covered entity of the breach. The purpose of this notification is to alert the covered entity to a breach so that the covered entity can begin preparations for providing individual notification and media notification, if required. In this notification, the business associate must provide, to the extent possible, a list to the covered entity of the individuals affected.

Finally, subject to § 164.414, covered entities have the burden of proof to establish that they are in compliance with the breach notification provisions. Additionally, § 164.530(j)(1)(iv) requires covered entities to provide sufficient documentation to meet this burden of proof.

3. Use of Improved Information Technology and Burden Reduction

The Act, and thus the final rule, permits the use of electronic media as a vehicle for providing individual notification. Section 164.404(d)(1)(i) of the final rule permits covered entities to provide individuals with notification of a breach via email if the individual agrees to receiving electronic notice and has not withdrawn the agreement. Additionally, covered entities that must provide substitute notification to individuals pursuant to § 164.404(d)(2)(ii) are given the option of providing this notification electronically on the home page of their web site.

With respect to a covered entity's obligation to notify the Secretary of breaches of unsecured protected health information under § 164.408, OCR intends to receive this information electronically. OCR is in the process of developing an automated process through which covered entities must report the required information electronically on the OCR web site.

4. Efforts to Identify Duplication and use of Similar Information

The Act and the final rule require covered entities to provide notification to individuals following a breach of unsecured protected health information. See § 164.404. Currently, most states have breach notification laws in place that require similar notification be made to affected individuals following a breach of security of personal information.

Because these laws apply only to personal information, many of these laws do not require notification following the breach of protected health information, and even in cases where a breach of protected health information would trigger notification under state law, we believe that both the state law notification and the notification under this rule can be satisfied with a single breach notification. Therefore, the notification requirements in this final rule are not duplicative.

With respect to the notification to the Secretary as required by the Act and § 164.408 of the final rule, prior to the Act covered entities were not required to report this information to OCR, however, many covered entities may have collected this information to comply with the HIPAA Privacy and Security Rules. Covered entities are now obligated to provide OCR with that information to comply with the Act and this final rule. Additionally, OCR must collect this information from covered entities to fulfill its obligation to provide Congress with annual reports of breaches that occur pursuant to § 13402(i) of the Act.

5. Impact on Small Businesses or Other Small Entities

This information collection affects all covered entities and business associates, regardless of their size. However, the burden upon covered entities and business associates to provide the appropriate notifications occurs only when there has been a breach of unsecured protected health information. Covered entities and business associates have no obligations under the Act or the final rule in the absence of a breach of unsecured protected health information.

With respect to the individual notification required by § 164.404 of the final rule, if a breach occurs at a small covered entity, it may be likely that there would be fewer affected individuals than at a larger covered entity. In that case, the burden and cost of notification would be relative to the covered entity's size and would not adversely affect small entities. If there is insufficient contact information for less than 10 individuals, the final rule attempts to minimize the burden for smaller covered entities by permitting some flexibility with the notification mechanism, as long as it is reasonably calculated to reach the affected individuals. Additionally, if substitute notice must be provided to 10 or more individuals, small covered entities must provide this notice on their web site or provide notice in major print or broadcast media. If a small entity does not have a web site, they are obligated to provide notice in major print or broadcast media that is reasonably calculated to reach affected individuals. Again, as small covered entities are likely to serve smaller geographic regions and fewer individuals than larger entities, there is some flexibility with respect to what media the covered entity uses to provide this substitute notice.

With respect to notification to the media following breaches affecting 500 or more individuals of a State or jurisdiction, pursuant to § 164.406, the burden upon small covered entities will be minimal. While possible, it is unlikely that small covered entities will experience breaches of this magnitude due to their small size, thus, notification to the media will rarely be required. Similarly, because the breaches experienced by small covered entities are unlikely to affect 500 or more individuals, small covered entities will

likely need only to provide the Secretary with an annual notice of all breaches that occurred in the past calendar year. See § 164.408.

Finally, with respect to small business associates, because business associates have only the burden of notifying the covered entity of a breach and not the affected individuals, this does not impose any adverse affect on small business associates. See § 164.410.

6. Consequences of Collecting the Information Less Frequently

With respect to the individual and media notices under §§ 164.404 and 164.406, the statute requires that covered entities provide these notifications following every breach of unsecured protected health information. Therefore, the statute provides no opportunity to provide notification less frequently.

Similarly, with respect to providing notice to the Secretary under § 164.408, the statute dictates that, at a minimum, covered entities provide notification of breaches affecting 500 or more individuals to the Secretary immediately and notification of breaches affecting less than 500 individuals annually. Again, the statute provides no flexibility in permitting us to collect this information less frequently.

7. Special Circumstances Relating to the Guidelines of 5 CFR 1320.5

There are no special circumstances.

8. Comments in Response to the Federal Register Notice/Outside Consultation

A 14-day Federal Register Notice was published in the Federal Register on August 24, 2009 (74 FR 42740). We received one general comment, in which the commenter suggested that, based on its experience, the Department had underestimated the burden of breach notification. The commenter did not provide any information to support its contention that the burden estimate is low, nor did the commenter provide an alternative burden estimate for our consideration. We believe that the commenter may be referencing the cost of putting in place security systems to prevent breaches from occurring; however, such systems are beyond the scope of this new breach reporting burden and should already be in place to ensure compliance with the HIPAA Privacy and Security Rules. We will take the comment into consideration as we develop our final regulations.

9. Explanation of any Payment/Gift to Respondents

Respondents will not receive any payments or gifts.

10. Assurance of Confidentiality Provided to Respondents

With respect to the information regarding breach of unsecured protected health information affecting more than 500 individuals, which must be submitted to the Secretary under § 164.408, there is no assurance of confidentiality because the Act requires this information to be posted on the HHS web site for the public to view. Additionally, OCR must submit information reported to the Secretary by covered entities regarding breaches of unsecured protected health information to Congress annually.

11. Justification for Sensitive Questions

This information collection does not require any sensitive information.

12. Estimates of Annualized Burden Hours (Total Hours & Wages)

12A. Estimated Annualized Burden Hours

Type of Respondent	Number of Respondents	Average Number of Responses per Respondent	Average Burden hours per Response	Total Burden Hours
Individual Notice—Written and E-mail Notice (drafting, preparing, sending, and documenting notification)	**106**	**1**	**206**	**21,836**
500 or More Affected Individuals (investigating and documenting breach)	**56**	**1**	**44**	**2,464**
Less than 500 Affected Individuals (investigating and documenting breach)	**50**	**1**	**8**	**400**
Individual Notice—Substitute Notice (posting or publishing)	**70**	**1**	**1**	**70**
Individual Notice—Substitute Notice (toll-free number)	**70**	**1**	**3,438**	**240,660**
Media Notice	**56**	**1**	**1**	**56**
Notice to Secretary (notice for breaches affecting 500 or more individuals and annual notice and maintenance of annual log)	**106**	**1**	**140/60**	**247**
TOTAL				**265,733**

To determine the total burden hours of providing the required notifications following a breach of unsecured protected health information, we relied on the information available at DataLossdb.org. We examined DataLossdb.org data relating to breaches from medical firms or containing medical information covering calendar year 2008.[1] In addition to the

[1] Using the data from DataLossdb.org, there is no way to determine how many of these breaches involved business associates rather than covered entities. Therefore, because business associates have significantly less responsibility following a breach than covered entities, such that business associates are only required to notify the covered entity of the breach and not to provide notification to affected individuals, the burden hours for business associates are encompassed in the calculations for covered entities.

information from DataLossdb.org, we relied on our experience implementing the HIPAA Privacy Rule to estimate the amount of time it will take covered entities to comply with these notification requirements.

From the DataLossdb.org information, we were able to estimate that 106 breaches will occur per year, affecting 2,888,804 individuals. Of these 106 breaches, 56 will affect 500 or more individuals such that media notice and immediate notice to the Secretary are required under §§ 164.406 and 164.408, while 70 breaches will likely require covered entities to send substitute notice under § 164.404(d)(2).

With respect to individual notice, when a breach occurs we expect a covered entity to spend time investigating the breach, drafting, preparing, and documenting the required notifications, and mailing or sending these notifications. Based on our estimates, approximately 106 breaches of unsecured protected health information will occur each year for which individual notification via written notice or e-mail notice will be required. We have divided the number of affected individuals by the number of breaches to obtain an average number of written or e-mail notices a covered entity would be required to send to individuals following a breach. On average, for each of the 106 breaches, a covered entity would need to provide notification to 27,253 affected individuals.

Totaling these burden hour estimates, the total burden hours upon covered entities for this information collection to be 265,733 hours. (See Attachment A for calculations.)

12B. Estimated Annualized Cost to Respondents

Type of Respondent	**Total Burden Hours**	**Hourly Wage Rate**	**Total Respondent Costs**
Individual Notice—Written and E-mail Notice (drafting, preparing, sending, and documenting notification)	**21,836**	**$30.00**	**$655,080**
500 or More Affected Individuals (investigating and documenting breach)	**2,640**	**$50.00**	**$123,200**
Less than 500 Affected Individuals (investigating and documenting breach)	**400**	**$50.00**	**$20,000**
Individual Notice—Substitute Notice (posting and publishing)	**70**	**$30.00**	**$2,100**
Individual Notice—Substitute Notice (toll-free number)	**240,660**	**$30.00**	**$7,219,800**
Media Notice	**56**	**$30.00**	**$1,680**
Notice to Secretary (notice for breaches affecting 500 or more	**244**	**$30.00**	**$7,410**

individuals and annual notice and maintenance of annual log)			
Total			**$8,029,270**

The total cost to respondents is $8,029,270. Using the total burden hours derived above for each type of notification required following a breach of unsecured protected health information, we multiplied that by $30.00, which is the median hourly wage for a healthcare practitioner and technical worker in 2008.[2] We have used $50.00 as the average for an office manager's median hourly wage.

13. Estimates of Other Total Annual Cost Burden to Respondents or Recordkeepers

Cost Elements	Number of Breaches	Cost per Breach	Total Cost
Individual Notice —Postage, Paper, and Envelopes	**106**	**$6,813**	**$722,178**
Individual Notice —Substitute Notice Media Posting	**70**	**$487**	**$34,090**
Individual Notice —Substitute Notice—Toll-Free Number	**70**	**$14,504**	**$1,015,280**
Media Notice— Posting or Publishing Notice	**56**	**$45**	**$2,520**
Total			**$1,774,068**

This table shows the estimated capital and maintenance costs to covered entities for providing the required breach notification.

The total capital and maintenance cost for covered entities providing the required breach notifications is $1,774,068. (See Attachment B for calculations.)

We have not included any capital or maintenance costs with respect to providing notice to the Secretary under § 164.408. These reports will be submitted electronically by filling out a form on the HHS web site. We have included discussion of the burden hours for collecting the appropriate information, submitting the electronic report, and maintaining the annual log of breaches above.

14. Annualized Cost to Federal Government

[2] Department of Labor, Occupational Employment Statistics; Healthcare Practitioner and Technical Occupations. http://www.bls.gov/oes/

The cost of providing these notifications falls upon covered entities and business associates. OCR does not produce or provide covered entities or business associate with the required notifications, store this information, or require covered entities to provide all information they collect to comply with these notification requirements to OCR. This portion of the collection is done outside of OCR and is a function completed entirely by the covered entities and business associates. Therefore, there is no cost to the federal government for this portion of the information collection.

OCR is required, however, to post on an HHS web site a list of the covered entities that have experienced breaches affecting more than 500 individuals. Additionally, OCR will also develop and maintain a database to receive reports of breaches from covered entities. Therefore, the annualized cost to the federal government will be approximately $500,000.

15. Explanation for Program Changes or Adjustments

This is a new data collection.

16. Plans for Tabulation and Publication and Project Time Schedule

The only portion of this information collection that will be published are the notifications provided by covered entities to the Secretary. The Act requires that breaches reported to the Secretary affecting 500 or more individuals be posted on the HHS web site. This information will be posted following the first report from a covered entity of such a breach. This list will be updated as additional reports from covered entities are received. Additionally, OCR is required to provide Congress with an annual report of all breaches for which the Secretary receives notification under § 164.408.

17. Reason Display of OMB Expiration Date is Inappropriate

The OMB expiration date may be displayed.

18. Exceptions to Certification for Paperwork Reduction Act Submissions

There are no exceptions to the certification.

B. Collection of Information Employing Statistical Methods

Not applicable. The information collection required above in part A does not require nor lend itself to the application of statistical methods.