Supporting Statement for
Breach Notification for Unsecured Protected Health Information
and Supporting Regulations Contained in
45 CFR Parts 160 and 164

A. Justification

1. Circumstances Making the Collection of Information Necessary

We are requesting OMB approval on the revision of a current information collection (OMB # 0945-0001; formerly 0990-0346). Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act requires OCR to collect information regarding breaches discovered by covered entities and their business associates under the HIPAA Privacy Rule. The final HIPAA Breach Notification Rule requires HIPAA covered entities to notify affected individuals, the Secretary, and, in some cases, the media of a breach of unsecured protected health information.

2. Purpose and Use of Information Collection

Pursuant the HIPAA Breach Notification Rule and the current information collection, 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; in situations in which a breach affects more than 500 individuals in a particular State or jurisdiction, a prominent media outlet serving that State or jurisdiction; and the Secretary of HHS. If a business associate discovers a breach, the Rule requires the business associate to notify the covered entity of the breach. Covered entities have the burden of proof to establish that they are in compliance with the breach notification provisions, and are required to provide sufficient documentation to meet this burden of proof. The Rule does not specify a required format for documentation.

3. Use of Improved Information Technology and Burden Reduction

The HIPAA Breach Notification Rule permits the use of electronic media as a vehicle for providing individual notification. The Breach Notification Rule permits covered entities to provide individuals with notification of a breach via email if the individual agrees to electronic notice and has not withdrawn the agreement. Additionally, covered entities that must provide substitute notification 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, OCR intends to continue receiving this information electronically.

4. Efforts to Identify Duplication and Use of Similar Information

Most states have breach notification laws in place that require similar notification to be made to affected individuals following a breach of security of personal information. However, many of these laws do not specifically 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.

5. Impact on Small Businesses or Other Small Entities

With regard to the HIPAA Breach Notification Rule, 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 HITECH Act or the final rule in the absence of a breach of unsecured protected health information.

Pursuant to HITECH, with respect to the individual notification required by the Breach Notification Rule, if a breach occurs at a small covered entity, there likely 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 fewer 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, it is 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 more than 500 individuals of a State or jurisdiction, 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.

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.

6. Consequences of Collecting the Information Less Frequent Collection

The HITECH Act requires that covered entities provide notifications following every breach of unsecured protected health information. Therefore, the statute provides no opportunity to provide notification 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 60-day Federal Register Notice was published in the Federal Register on October 9, 2009 (74 FR 52235). We did not receive any comments in response to the publication, and the information collection requirements were adopted in the HIPAA Breach Notification Rule,

which was published on January 25, 2013, as part of the Omnibus HIPAA Final Rule (78 FR 5566).

9. Explanation of Any Payment/Gift to Respondents

There are no payments or gifts to the respondents.

10. Assurance of Confidentiality Provided to Respondents

The HIPAA Privacy and Security Rules require covered entities and business associates to protect individually identifiable health information. With respect to the information regarding breach of unsecured protected health information affecting 500 or more individuals, there is no assurance of confidentiality because the HITECH Act requires this information to be posted on the HHS web site for the public to view.

11. Justification for Sensitive Questions

The federal government does not require that sensitive questions be asked in this information collection.

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

The overall total for respondents to comply with the information collection requirements of the Breach Notification Rule is 236,196 burden hours. In addition, we estimate a voluntary burden to individuals of approximately 82,569 hours, resulting in a total of 318,765 burden hours associated with the rule. Details are presented below.

12A. Estimated Annualized Burden Hours

Section	Type of Respondent	Number of Respondents	Average Number of Responses per Respondent	Average Burden hours per Response	Total Burden Hours
164.404	Individual Notice—Written and E-mail Notice (drafting)	19,000	1	.5	9,500
164.404	Individual Notice—Written and E-mail Notice (preparing and documenting notification)	19,000	1	.5	9,500
164.404	Individual Notice—Written and E-mail Notice (processing and sending)	19,000	353	.008	53,656
164.414	500 or More Affected Individuals (investigating and documenting breach)	250	1	50	12,500
164.414	Less than 500 Affected Individuals (investigating and documenting breach)	940 (affecting 10-499 individuals)	1	8	7,520
		17,810 (affecting <10 individuals)	1	4	71,240
164.404	Individual Notice—Substitute Notice (posting or publishing)	1,190	1	1	1,190
164.404	Individual Notice—Substitute Notice (setting up and staffing toll-free number)	1,190	1	46.26	55,049
164.404	Individual Notice—Substitute Notice (individual burden to call toll-free number for information)	660,550	1	7.5/60	82,569
164.406	Media Notice	250	1	1.25	313
164.408	Notice to Secretary (notice for breaches affecting 500 or more individuals)	250	1	1.25	313
164.408	Notice to Secretary (notice for breaches affecting fewer than 500 individuals)	18,750	1	1	18,750
Total					**322,100**

12B. Estimated Annualized Burden Costs

The Breach Notification Rule implements the HITECH Act requirements for covered entities to notify individuals, HHS, and in some cases, the media, in the case of a breach of unsecured protected health information.

To determine the total burden hours of providing the required notifications following a breach of unsecured protected health information, we relied on our experience receiving breach notifications during calendar years 2010 and 2011 and our experience implementing the Privacy Rule to estimate the amount of time and associated cost to covered entities to comply with these notification requirements. We estimate that in general 19,000 breaches will occur per year, affecting 6,710,000 individuals. Of these 19,000 breaches, 250 will affect enough individuals that media notice (more than 500 individuals affected) and immediate notice to the Secretary (500 or more individuals affected) are required under §§ 164.406 and 164.408, while 1,190 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 19,000 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 19,000 breaches, a covered entity would need to provide notification to 353 affected individuals.

The total burden hours upon covered entities for compliance the Breach Notification Rule is estimated to be 236,196 hours. The activities constituting this burden are outlined in the table above. We multiplied the total burden hours derived above by the hourly wage rates provided in our impact analysis. In addition, we estimated the total burden hours to individuals choosing to take advantage of the opportunity to call the toll-free line for more information and multiplied those hours by the average hourly wage for all occupations. The total cost to respondents (including covered entities and individuals) of the burden hours for compliance with the Breach Notification Rule is approximately $11.6 million.

12B. Estimated Annualized Cost to Respondents

Section	Type of Respondent	Total Burden Hours (rounded)	Hourly Wage Rate	Total Respondent Costs
164.404	Individual Notice—Written and E-mail Notice (drafting)	9,500	$42.96[1]	$408,120
164.404	Individual Notice—Written	9,500	$22.53[2]	$214,035

[1] Department of Labor, Occupational Employment Statistics. The median hourly wage for the Healthcare Practitioner and Technical Occupations labor category is $28.64, to which we add 50 percent to account for benefits, resulting in an hourly wage rate of $42.96. Available at http://www.bls.gov/oes/current/oes_nat.htm.

[2] The median hourly wage for Office and Administrative Support Occupations is $15.02 per hour, to which we add 50 percent for benefits, resulting in an hourly wage rate of $22.53.

	and E-mail Notice (preparing and documenting notification)			
164.404	Individual Notice—Written and E-mail Notice (processing and sending)	53,656	$22.53[3]	$1,208,870
164.414	500 or More Affected Individuals (investigating and documenting breach)	12,500	$67[4]	$837,500
164.414	Less than 500 Affected Individuals (investigating and documenting breach)	7,520 (for breaches affecting <10 individuals)	$67[5]	$503,840
		71,240 (for breaches affecting 10-299 individuals)	$67	$4,773,080
164.404	Individual Notice—Substitute Notice (staffing toll-free number)	55,049	$22.53[6]	$1,240,254
164.404	Individual Notice—Substitute Notice (individuals burden to call toll-free number for information)	82,569	$24.86[7]	$2,052,665
164.406	Media Notice	313	$49.34[8]	$15,443
164.408	Notice to Secretary (notice for breaches affecting 500 or more individuals)	313	$49.34	$15,443
164.408	Notice to Secretary (notice for breaches affecting fewer than 500 individuals)	18,750	$22.53[9]	$422,438

[3] The hourly wage rate for office workers and administrative support staff is $22.53.
[4] We estimate the hourly wage rate for an office manager is approximately $67 ($44.65 median wage for All Management Occupations plus 50% for benefits).
[5] The hourly wage rate for an office manager is $67.
[6] The hourly wage rate for office workers and administrative support staff is $22.53.
[7] The median compensation amount for all occupations is $24.86 ($16.57 plus 50% to account for fringe benefits). Available at http://www.bls.gov/oes/current/oes_nat.htm#00-0000.
[8] As explained in the regulatory impact analysis published with the final rule, the cost of media notice and of notice to the Secretary of breaches affecting 500 or more individuals includes: (i) one hour of an equivalent to a GS-12 Federal employee earning $43.50 per hour to draft the notice ($29 per hour plus 50% for benefits), and (ii) one quarter of an hour for a public relations manager or their equivalent, at $67.29 per hour ($44.86 plus 50% for benefits) to approve the release/report. For purposes of this ICR, we used the total annual cost and the number of anticipated notices/reports to estimate an average hourly wage for these activities of $49.34 (including benefits).
[9] The hourly wage rate for office workers and administrative support staff is $22.53.

Total				**$11,691,688**

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

Section	Cost Elements	Number of Breaches	Cost per Breach	Total Cost
164.404	Individual Notice—Postage, Paper, and Envelopes	**19,000**	**$90**	**$1,710,000**
164.404	Individual Notice—Substitute Notice Media Posting	**1,190**	**$480**	**$571,200**
164.404	Individual Notice—Substitute Notice—Toll-Free Number	**1,190**	**$484**	**$575,960**
Total				**$2,857,160**

This table shows the estimated capital and maintenance costs to covered entities for providing breach notification as required by the Breach Notification Rule. The total capital and maintenance cost for covered entities providing the required breach notifications is $2,857,160. We have not included any capital or maintenance costs with respect to providing notice to the Secretary. These reports will be submitted electronically by filling out a form on the HHS web site. We have included estimates 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

The cost of providing breach 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 500 or more 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 data collection is ongoing. OCR has adjusted upward the estimated number of respondents and responses, and, as a result, adjusted the annual hour burden from 265,733 to 318,765 and the annual cost burden from $1,774,068 to $14,474,969 (including capital and other costs). The revisions to the current information collection are due to information learned about the volume and nature of breaches that occur from our actual experience in administering the breach notification requirements under the interim final rule. In addition, costs have increased due to upward adjustments in hourly wage rates since the previous information collection.

16. Plans for Tabulation and Publication and Project Time Schedule

There are no plans for tabulation or publication.

17. Reason(s) 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 by the HIPAA Privacy, Security, and Breach Notification Rules as described above in part A do not require the application of statistical methods.