**Supporting Statement for**

**HIPAA Privacy, Security, and Breach Notification Rules,**

**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 for the revision of a previously approved Office for Civil Rights (OCR) data collection, OMB #0945-0003 (currently named Privacy Standards and Supporting Regulations). There are no program changes associated with this revision. Specifically, we request approval to update the burden estimates for the information collection and incorporate into it the substance of two other previously approved OCR data collections, OMB#0945-0001 (Breach Notification) and OMB#0945-0004 (Security Standards), with revisions described below. At the same time that the revised, consolidated data collection is approved, we request that the data collections numbered #0945-0001 and #0945-0004 be discontinued. Consolidation into one master information collection that includes all applicable regulatory requirements of the HIPAA Privacy, Security, and Breach Notification Rules will allow the public, the regulated community, and OCR to more easily view and track the estimated burdens associated with the suite of HIPAA regulations that are administered and enforced by OCR.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA),[1] the Health Information Technology for Economic and Clinical Health (HITECH) Act),[2] and their implementing regulations at 45 CFR Parts 160 and 164--the HIPAA Privacy, Security, and Breach Notification Rules--establish requirements for covered entities (health plans, health care clearinghouses, and most health care providers) and their business associates with respect to individuals' health information. The HIPAA Rules require covered entities, and in many respects their business associates, to protect the privacy and security of individually identifiable health information (called "protected health information" or "PHI"); fulfill individuals' rights under HIPAA with respect to their health information; and notify affected individuals, the Secretary, and in some cases the media of a breach of unsecured protected health information.

The HITECH Act also requires OCR to collect information regarding breaches discovered by covered entities and their business associates.

**2. Purpose and Use of Information Collection**

The information collection for the HIPAA Privacy Rule addresses HIPAA requirements related to the use, disclosure, and safeguarding of individually identifiable health information by covered entities affected by the Rule. The information is routinely used by covered entities and business associates for treatment, payment, and health care operations. In addition, the information is used for specified public policy purposes, including research, public health, and as required by other laws. The Privacy Rule also ensures that individuals are able to exercise certain rights with respect to their information, including the rights to access and seek amendments to

[1] Public Law 104-191,
[2] The HITECH Act is Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Public Law 111–5).

their health records and to receive a Notice of Privacy Practices (NPP) from their direct treatment providers and health plans.

As noted above, we modify this information collection to incorporate the HIPAA Security Rule's requirements that covered entities and business associates maintain reasonable and appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and availability of electronic information and to protect against any reasonably anticipated threats or hazards to the security of the information and prevent unauthorized use or disclosure of the information. Covered entities and business associates are required to produce documentation to demonstrate the implementation of reasonable and appropriate safeguards when asked by OCR.

In addition, we modify this information collection to incorporate requirements of the HIPAA Breach Notification Rule, which requires covered entities to 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. 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.

Finally, we modify this information collection to incorporate the HITECH Act's requirement that OCR post on its website information about breaches of protected health information affecting 500 or more individuals.

**3. Use of Improved Information Technology and Burden Reduction**

The HIPAA Privacy, Security, and Breach Notification Rules were constructed to allow covered entities at different levels of technological sophistication to be able to adapt their existing systems to the requirements of the regulations. Thus, covered entities are able to determine for themselves the appropriate level of technology and implement safeguards in a manner that is reasonable and appropriate for their particular environments. The Privacy Rule allows entities covered by HIPAA to provide the required notice of privacy practices to an individual by email, if the individual agrees to notice in an electronic format, and such agreement has not been withdrawn. In addition, covered entities may provide individuals with the opportunity to make requests for their information electronically and generally are required to provide individuals with access to their information in electronic form if requested by the individual.

The Security Rule applies only to entities that maintain electronic protected health information. HIPAA covered entities and business associates that are subject to the Security Rule's requirements are permitted to maintain the required documentation in electronic or paper form.

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**

The information collection requirements of the HIPAA Privacy and Security Rules do not duplicate those of any other federal regulation. The Security Rule's standards for safeguarding electronic information are consistent with best practices in the industry, and certain other requirements, such as those provided by the Federal Trade Commission, may be similar to certain Security Rule requirements. In such cases, the activities performed in compliance with other security frameworks likely would fulfill an equivalent Security Rule requirement, and thus the Security Rule does not create an additional burden in this respect. In contrast, the documentation requirements of the Security Rule are specific to the Security Rule and do not duplicate other laws.

With respect to the HIPAA Breach Notification Rule, 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 the HIPAA Breach Notification Rule are not duplicative.

**5. Impact on Small Businesses or Other Small Entities**

The HIPAA Privacy and Security Rules provide great flexibility to covered entities and business associates, including small businesses, to determine the policies and procedures that are best suited to the entities' current practices to comply with the standards, implementation specifications and requirements of the Rules. The Rules generally provide a flexible and scalable approach to appropriate methods for compliance depending on the size and capabilities of each individual covered entity and business associate.

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 Breach Notification Rule in the absence of a breach of unsecured protected health information. Further, covered entities and business associates can avoid Breach Notification obligations altogether by implementing appropriate protections for protected health information in accordance with the HIPAA Privacy and Security Rules.

**6. Consequences of Less Frequent Collection**

Under the HIPAA Privacy and Security Rules, the frequency of collection is a function of activity by covered entities and business associates and the policies and procedures that they establish for complying with the Rules, and of the need for the Department to examine the entities' policies and procedures for compliance and enforcement purposes, such as to evaluate a complaint against a covered entity or business associate. With respect to the Breach Notification Rule, 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 notice was published in the Federal Register on March 17, 2016 (81 FR 14453). No public comments were received. A 30-day notice was published on May 19, 2016 (81 FR 31646).

**9. Explanation of Any Payment/Gift to Respondents**

There are no payments or gifts to the respondents.

**10. Assurance of Confidentiality Provided to Respondents**

OCR complies with the Privacy Act of 1974 (5SUC 552a) and the Freedom of Information Act (5 CFR 552) with respect to information provided to OCR. With respect to information regarding

breaches of unsecured protected health information affecting 500 or more individuals, there is no assurance of confidentiality made to the covered entities and business associates involved 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 HIPAA Privacy, Security, and Breach Notification Rules is 921,813,702 burden hours at a cost of $57,678,383,579. Details are presented below.

**12A. Estimated Annualized Burden Hours**

For ease of reference, footnotes attached to the table below indicate how certain of the estimated numbers were calculated, although the formulas and assumptions behind many of the estimates remain unchanged since the previously approved information collections issued in conjunction with the Omnibus HIPAA Final Rule.[3] As we have done in our previous regulatory ICRs, we sometimes count the "number of respondents" as the number of entities subject to a regulatory requirement and in other cases provide an estimate of individuals who are affected by entities'

[3] See 78 FR 5566 (January 25, 2013).

compliance activities, or who make use of a provision to exercise an individual right under the Rules. Although we believe this makes the calculations more transparent, it is not always obvious for any given provision which individuals or entities constitute the "respondents," so we indicate this in the table where appropriate. The estimated burden of a provision accrues to covered entities and/or business associates for all but one burden category, where we indicate that the (voluntary) burden applies to individuals.

See the narrative in item 15 for an explanation of adjustments related to the ongoing collection burdens and costs below.

Ongoing Annual Burdens of Compliance with the Rules

| **Section** | **Type of Respondent** | **Number of Respondents** | **Number of Responses per Respondent** | **Average Burden hours per Response[4]** | **Total Burden Hours** |
|---|---|---|---|---|---|
| 160.204 | Process for Requesting Exception Determinations (states or persons) | 1 | 1 | 16 | 16 |
| 164.308 | Risk Analysis - Documentation | 1,700,000[5] | 1 | 10 | 17,000,000 |

[4] The figures in this column are averages based on a range. Small entities may require fewer hours to conduct certain compliance activities, particularly with respect to Security Rule requirements, while large entities may spend more hours than those provided here.

[5] This estimate includes 700,000 estimated covered entities and 1 million estimated business associates. The Omnibus HIPAA Final Rule burden analysis estimated that there were 1-2 million business associates. However, because many business associates have business associate relationships with multiple covered entities, we believe the lower end of this range is more accurate.

| | | | | | |
|---|---|---|---|---|---|
| 164.308 | Information System Activity Review – Documentation | 1,700,000 | 12 | .75 | 15,300,000 |
| 164.308 | Security Reminders – Periodic Updates | 1,700,000 | 12 | 1 | 20,400,000 |
| 164.308 | Security Incidents (other than breaches) – Documentation | 1,700,000 | 52 | 5 | 442,000,000 |
| 164.308 | Contingency Plan – Testing and Revision | 1,700,000 | 1 | 8 | 13,600,000 |
| 164.308 | Contingency Plan – Criticality Analysis | 1,700,000 | 1 | 4 | 6,800,000 |
| 164.310 | Maintenance Records | 1,700,000 | 12 | 6 | 122,400,000 |
| 164.314 | Security Incidents – Business Associate reporting of incidents (other than breach) to Covered Entities | 1,000,000 | 12 | 20 | 240,000,000 |
| 164.316 | Documentation – Review and Update[6] | 1,700,000 | 1 | 6 | 10,200,000 |
| 164.404 | Individual Notice—Written and E-mail Notice (drafting) | 58,481[7] | 1 | .5 | 29,240 |
| 164.404 | Individual Notice—Written and E-mail Notice (preparing and documenting notification) | 58,481 | 1 | .5 | 29,240 |
| 164.404 | Individual Notice—Written and E-mail Notice | 58,481 | 353[8] | .008 | 165,150 |

[6] This element includes the burden of updating documentation in accordance with the evaluation required by 45 CFR 164.306. Therefore, we do not separately address the burden associated with the evaluation.
[7] Total number of breach incidents in 2015.
[8] Average number of individuals affected per breach incident in 2015.

| | | | | | |
|---|---|---|---|---|---|
| | (processing and sending) | | | | |
| 164.404 | Individual Notice—Substitute Notice (posting or publishing) | 2,746[9] | 1 | 1 | 2,746 |
| 164.404 | Individual Notice—Substitute Notice (staffing toll-free number) | 2,746 | 1 | 5.75[10] | 15,789 |
| 164.404 | Individual Notice—Substitute Notice (individuals' voluntary burden to call toll-free number for information) | 11,326,440[11] | 1 | .125[12] | 1,415,805 |
| 164.406 | Media Notice | 267[13] | 1 | 1.25 | 333 |
| 164.408 | Notice to Secretary (notice for breaches affecting 500 or more individuals) | 267 | 1 | 1.25 | 333 |
| 164.408 | Notice to Secretary (notice for breaches affecting fewer than 500 individuals) | 58,215[14] | 1 | 1 | 58,215 |

[9] This number includes all 267 large breaches and all 2,479 breaches affecting 10-499 individuals. As we stated in the preamble to the Omnibus HIPAA Final Rule, although some breaches involving fewer than 10 individuals may require substitute notice, we believe the costs of providing such notice through alternative written means or by telephone is negligible.

[10] We again assume that call center staff will spend 5 minutes per call, but now with an average of 4,124 individuals affected by breaches requiring substitute notice. Multiplying these figures results in 5.75 hours per breach. This estimate is much lower than the 46.26 hours per breach requiring substitute notice in our previous estimate, which we believe was the result of an arithmetic error. The estimate of 4,124 individuals being affected by breaches requiring substitute notice results from the assumption that the number of callers to the toll-free number will equal 10% of the sum of all individuals affected by large breaches (113,250,136) and 5% of individuals affected by small breaches (.05 x 285,413 = 14,270). We calculate .10 * (113,250,136 + 14,270) = 11,326,440.

[11] As noted in the previous footnote, this number equals 10% of the sum of all individuals affected by large breaches and 5% of individuals affected by small breaches.

[12] This number includes 7.5 minutes for each individual who calls: an average of 2.5 minutes to wait on the line/decide to call back and 5 minutes for the call itself.

[13] The total number of breaches affecting 500 or more individuals in 2015.

[14] The total number of breaches affecting fewer than 500 individuals in 2015.

| | | | | | |
|---|---|---|---|---|---|
| 164.414 | 500 or More Affected Individuals (investigating and documenting breach) | 267 | 1 | 50 | 13,350 |
| 164.414 | Less than 500 Affected Individuals (investigating and documenting breach) | 2,479 (breaches affecting 10-499 individuals) | 1 | 8 | 19,832 |
| | | 55,736 (breaches affecting <10 individuals) | 1 | 4 | 222,944 |
| 164.504 | Uses and Disclosures – Organizational Requirements | 700,000 | 1 | 5/60 | 58,333 |
| 164.508 | Uses and Disclosures for Which Individual authorization is required | 700,000 | 1 | 1 | 700,000 |
| 164.512 | Uses and Disclosures for Research Purposes | 113,524[15] | 1 | 5/60 | 9,460 |
| 164.520 | Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by paper mail) | 100,000,000[16] | 1 | 0.25 minutes [1 hour per 240 notices] | 416,667 |
| 164.520 | Notice of Privacy Practices for Protected Health Information (health plans – | 100,000,000 | 1 | 0.167 minutes [1 hour per 360 notices] | 278,333 |

[15] The number of entities who use and disclose protected health information for research purposes.
[16] As in our previous submission, we assume that half of the approximately 200,000,000 individuals insured by covered health plans will receive the plan's NPP by paper mail, and half will receive the NPP by electronic mail.

| | | | | | |
|---|---|---|---|---|---|
| | periodic distribution of NPPs by electronic mail) | | | | |
| 164.520 | Notice of Privacy Practices for Protected Health Information (health care providers – dissemination and acknowledgement) | 613,000,000[17] | 1 | 3/60 | 30,650,000 |
| 164.522 | Rights to Request Privacy Protection for Protected Health Information | 20,000[18] | 1 | 3/60 | 1,000 |
| 164.524 | Access of Individuals to Protected Health Information (disclosures) | 200,000[19] | 1 | 3/60 | 10,000 |
| 164.526 | Amendment of Protected Health Information (requests) | 150,000 | 1 | 5/60 | 12,500 |
| 164.526 | Amendment of Protected Health Information (denials) | 50,000 | 1 | 5/60 | 4,166 |
| 164.528 | Accounting for Disclosures of Protected Health Information | 5,000[20] | 1 | 3/60 | 250 |
| **Total** | | | | | **921,813,702** |

[17] We estimate that each year covered health care providers will have first-time visits with 613 million individuals, to whom the providers must give a NPP.
[18] We assume covered entities address 20,000 requests for confidential communications or restrictions on disclosures per year.
[19] We estimate that covered entities annually fulfill 200,000 requests from individuals for access to their protected health information.
[20] We estimate that covered entities annually fulfill 5,000 requests from individuals for an accounting of disclosures of their protected health information.

**12B. Estimated Annualized Burden Costs**

The total cost of this information collection, apart from capital costs, is approximately $57,678,383,579.

Ongoing Annual Burden Costs

| Section | Type of Respondent | Total Burden Hours | Hourly Wage Rate | Total Respondent Costs |
|---|---|---|---|---|
| 160.204 | Process for Requesting Exception Determinations (states or persons) | 16 | $44.50[21] | $687 |
| 164.308 | Risk Analysis - Documentation | 17,000,000 | $64.11[22] | $1,089,870,000 |
| 164.308 | Information System Activity Review – Documentation | 15,300,000 | $64.11 | $980,883,000 |
| 164.308 | Security Reminders – Periodic Updates | 20,400,000 | $64.11 | $1,307,844,000 |
| 164.308 | Security Incidents (other than breaches) – Documentation | 442,000,000 | $64.11 | $28,336,620,000 |
| 164.308 | Contingency Plan – Testing and Revision | 13,600,000 | $64.11 | $871,896,000 |
| 164.308 | Contingency Plan – Criticality Analysis | 6,800,000 | $64.11 | $435,948,000 |
| 164.310 | Maintenance Records | 122,400,000 | $58.33[23] | $7,139,592,000 |
| 164.314 | Security Incidents – Business Associate reporting of incidents (other than breach) to | 240,000,000 | $64.11 | $15,386,400,000 |

[21] The $44.50 wage, which includes $29.67 plus 50% for benefits, applies to the category "Healthcare Practitioners and Technical Workers."
[22] The $64.11 wage, which includes $42.74 plus 50% for benefits, applies to the category "Information Security Analysts."
[23] The $58.33 wage, which includes $38.89 plus 50% for benefits, applies to "Management Analysts."

| | | | | |
|---|---|---|---|---|
| | Covered Entities | | | |
| 164.316 | Documentation – Review and Update | 10,200,000 | $64.11 | $653,922,000 |
| 164.404 | Individual Notice—Written and E-mail Notice (drafting) | 29,240 | $44.50 | $1,301,180 |
| 164.404 | Individual Notice—Written and E-mail Notice (preparing and documenting notification) | 29,240 | $23.46[24] | $685,970 |
| 164.404 | Individual Notice—Written and E-mail Notice (processing and sending) | 165,150 | $23.46 | $3,874,419 |
| 164.404 | Individual Notice—Substitute Notice (posting or publishing) | 2,746 | $73.20[25] | $201,007 |
| 164.404 | Individual Notice—Substitute Notice (staffing toll-free number) | 15,789 | $23.46 | $370,409 |
| 164.404 | Individual Notice—Substitute Notice (individuals burden to call toll-free number for information) | 1,415,805 | $25.63[26] | $36,287,082 |
| 164.406 | Media Notice | 333 | $50.29[27] | $16,749 |
| 164.408 | Notice to Secretary (notice for breaches affecting 500 or more individuals) | 333 | $50.29 | $16,749 |
| 164.408 | Notice to Secretary (notice for breaches affecting fewer than 500 individuals) | 58,215 | $23.46 | $1,365,723 |
| 164.414 | 500 or More Affected Individuals (investigating and documenting breach) | 13,350 | $70.12[28] | $936,102 |
| 164.414 | Less than 500 Affected Individuals (investigating and documenting breach) | 19,832(for breaches affecting <10 individuals) | $70.12 | $1,390,619 |

[24] The $23.46 wage, including $15.64 plus 50% for benefits, applies to "Office and Administrative Support Occupations."
[25] The $73.20 wage, including $48.80 plus 50% for benefits, applies to "Public Relations Managers."
[26] The $25.63 wage, including $17.09 plus 50% for benefits, is the median wage for "All Occupations."
[27] The $50.29 average cost per hour is derived by calculating the cost for 267 hours for a GS-12 equivalent ($44.64 per hour) and 66 hours for a Public Relations Manager ($73.20 per hour).
[28] The $70.12 wage, including $46.75 plus 50% for benefits, applies to "Management Occupations."

| | | | | |
|---|---|---|---|---|
| | | 222,944(for breaches affecting 10-299 individuals) | $70.12 | $15,632,833 |
| 164.504 | Uses and Disclosures – Organizational Requirements | 58,215 | $44.50 | $2,595,818 |
| 164.508 | Uses and Disclosures for Which Individual authorization is required | 700,000 | $44.50 | $31,150,000 |
| 164.512 | Uses and Disclosures for Research Purposes | 9,460 | $44.50 | $420,970 |
| 164.520 | Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs, half by paper mail and half by electronic mail) | 695,000 | $23.46 | $9,775,007 |
| 164.520 | Notice of Privacy Practices for Protected Health Information (health care providers – dissemination and acknowledgement) | 30,650,000 | $44.50 | $1,363,925,000 |
| 164.522 | Rights to Request Privacy Protection for Protected Health Information | 1,000 | $44.50 | $44,500 |
| 164.524 | Access of Individuals to Protected Health Information (disclosures) | 10,000 | $44.50 | $445,000 |
| 164.526 | Amendment of Protected Health Information (requests) | 12,500 | $44.50 | $556,250 |
| 164.526 | Amendment of Protected Health Information (denials) | 4,166 | $44.50 | $185,387 |
| 164.528 | Accounting for Disclosures of Protected Health Information | 250 | $44.50 | $11,125 |
| **Total** | | | | **$57,678,383,579** |

**13. Estimates of Other Total Annual Cost Burden to Respondents or Record Keepers/Capital Costs**

The total capital and maintenance cost for covered entities providing the required breach notifications is $**112,901,350**. This estimate is increased due to the much higher number of breaches and individuals affected by breach incidents. Capital costs will also be incurred by respondents in connection with the need to print notices of privacy practices and in certain cases to mail the notices to the individual.

**Total Annual/Annualized Capital Costs**

| Section | Cost Elements | Number of Breaches | Cost per Breach | Total Cost |
|---|---|---|---|---|
| 164.404 | Individual Notice—Postage, Paper, and Envelopes | 58,482 | $533[29] | $31,170,906 |
| 164.404 | Individual Notice—Substitute Notice Media Posting | 2,746[30] | $480 | $1,318,080 |
| 164.404 | Individual Notice—Substitute Notice—Toll-Free Number | 2,746 | $1,534[31] | $4,212,364 |
| 164.520 | Printing and Postage for Notice of Privacy Practices for Protected Health Information (health plans) | 0 | 0 | $14,900,000[32] |
| 164.520 | Printing Notice of Privacy | 0 | 0 | $61,300,000[33] |

[29] We again assume that half of all affected individuals (half of 113,535,549 equals 56,767,774) would receive paper notification and half would receive notification by email. Therefore, on average, 970 individuals per breach will receive notification by mail. Further, we estimate that each mailed notice will cost $.06 for paper and envelope and $.49 for postage. On average, the capital cost for mailed notices for each breach is $.55 for each of 970 notices, or $533.

[30] The number of breaches requiring substitute notice, the formula for which is provided above with the tables showing costs for hourly burdens.

[31] This number includes $60 per breach for start-up and monthly costs, plus $.35 cents per call for 4,124 calls.

[32] This number results from the following assumptions: (1) only 10% of 100 million notices will be mailed separately from regular plan mailings; (2) Each of 10 million paper notices costs $.49 to mail, for a total of $4.9 million in postage costs; and (3) each of 100 million paper notices costs $.10 to print, for a total of $10 million in printing costs.

[33] This estimate includes 613 million notices with a printing cost of $.10 per notice. This is less than the previous estimate because we have deleted the one-time additional costs of off-cycle printing to comply with the Omnibus HIPAA Final Rule.

| | | | | |
|---|---|---|---|---|
| | Practices for Protected Health Information (health care providers) | | | |
| **Total** | | | | **$112,901,350** |

**14. Annualized Cost to Federal Government**

The HIPAA Privacy and Security Rules require covered entities and business associates to collect and maintain information in order to comply with the Rules' requirements. However, OCR does not produce the forms on which the information is collected, OCR does not store this information, nor does OCR require covered entities and business associates to provide OCR with all information they collect to comply with the Rules. Similarly, 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. The costs to covered entities and business associates that are Federal entities are included among the overall burden estimates for covered entities and business associates, and thus are not addressed here. There is otherwise 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. The initial posting of such breaches is now automated; however, OCR now drafts and posts summaries of each large breach on the

website. Additionally, OCR maintains a database to receive reports of breaches from covered entities. Therefore, the annualized cost to the federal government is approximately $300,000.

**15. Explanation for Program Changes or Adjustments**

We have not made program changes since the previous information collection submissions, and this information collection does not create any new requirements for regulated entities or individuals. As noted above, we have combined three existing information collections into a single collection addressing burdens associated with the HIPAA Privacy, Security, and Breach Notification Rules. In addition, we have made a number of adjustments to the estimated ongoing annual burdens to reflect our experience with the use of these provisions and increases in average wages for the applicable labor categories. Finally, we have deleted first year compliance burdens of the Omnibus HIPAA Final Rule; we are well past the compliance deadlines, so these burdens no longer apply. We address these adjustments below in order of the tables in 12A and 12B.

***45 CFR 164.308-316 (provisions of the HIPAA Security Rule)***

The previous ICR (OMB #0945-0004) included a limited number of Security Rule provisions and assumed that no costs would be associated with the estimated burden hours. Based on our experience with implementation of the HIPAA Security Rule, as well as our knowledge of best practices in the health care industry, we have identified additional areas of ongoing compliance burdens and revised the estimated Security Rule burdens accordingly. The revised burden also reflects the burden on business associates, which were not responsible for compliance at the time the Security Rule burden analysis was initially approved. We include additional provisions that

carry an annual information collection burden, estimate costs associated with the burden hours, and revise the estimated numbers of respondents. We also remove a burden associated with initial (rather than ongoing) compliance with the Security Rule (section 164.306 "Justification") and revise the descriptions of the remaining provisions to more clearly reference the applicable regulatory provisions. This information collection now estimates annual burdens of recordkeeping and reporting in the following areas:

- Documentation of an entity's analysis of risks to the security of the electronic protected health information it maintains
- Documentation of information system activity review (such as audit logs)
- Periodic security reminders/updates for workforce members
- Documentation of security incidents (other than breaches)
- Contingency plan testing and revision
- Documentation of the entity's analysis of the criticality of applications and data
- Records of maintenance activities to ensure facility security
- Business associate reporting of security incidents (other than breaches) to the covered entity
- Review and update of documentation of policies and procedures,[34] as well as documentation of other activities undertaken in compliance with the Security Rule

For most of these activities, all covered entities (approximately 700,000) and business associates (approximately 1 million) are respondents. Only business associates are listed as respondents for purposes of reporting incidents to the covered entity. We note that the estimated burdens reflect

[34] This includes updates based on the evaluation of policies and procedures required by 45 CFR 164.308. As such, the burden of the evaluation requirement is not separately addressed in this information collection.

our expectation that covered entities and business associates have a certain level of knowledge and experience because the Security Rule has been in effect since 2003, and business associates have been directly subject to the Security Rule since 2013. The compliance activities listed occur annually (1 response), monthly (12 responses), or weekly (52 responses), as shown in the table above. As indicated in footnotes to the cost estimate table, we assume that most of the activities will be done by an information security analyst; in one case, we assume that a management analyst will perform the activity.

As a result of all of these changes, the estimated burdens of the Security Rule are significantly increased. In fact, the Security Rule burden analysis likely overestimates burden hours and costs in some respects, because certain of the information collection requirements are best practices and required or recommended by other security frameworks, and thus are part of the baseline. Nevertheless, we acknowledge the costs because we do not know the extent to which entities create specific Security Rule documentation separate from the documentation of information security activities that are otherwise part of the cost of doing business, apart from any Security Rule requirements.

Finally, we delete the one-time burdens and associated costs for certain Security Rule provisions that were included in this information collection (OMB #0945-0003) as part of the initial implementation of the Omnibus HIPAA Final Rule.

The total estimated annual costs associated with Security Rule information collection requirements have increased from $0 to $56,202,925,000.

***45 CFR 164.404-414 (provisions of the HIPAA Breach Notification Rule)***

The burden hours associated with the Breach Notification Rule also are significantly greater than what was indicated in the previous information collection (OMB #0945-0001). We have increased the numbers of breach incidents and individuals affected by breaches of their protected health information based on our experience with the breach notification program. The numbers in the table reflect data from calendar year 2015.

The total estimated annual costs associated with compliance with the Breach Notification requirements have increased from $1,083,092 to $62,078,842.

***45 CFR 164.504-528 (provisions of the HIPAA Privacy Rule)***

We have revised some of the burden estimates associated with the Privacy Rule based on feedback from covered entities and the public, as well as our experience administering the Privacy Rule. The following sources of hourly burdens have increased:

- The number of requests from individuals to access their protected health information is increased from 150,000 to 200,000 annually, based on feedback indicating broad interest among individuals in obtaining their protected health information.
- We believe that covered entities spend approximately 10,000 hours per year, which is more than the previous estimate of 7,500 hours per year, addressing individuals' requests to amend their protected health information (whether by fulfilling or denying the request).

The following sources of hourly burden have decreased:

- We believe only 20,000 individuals, not 150,000 individuals, request confidential communications or restrictions on disclosures of protected health information.
- We believe covered entities receive a total of only 5,000 requests for an accounting of disclosures per year, not 70,000.
- In addition, we have removed from this information collection the one-time burdens associated with initial implementation of the Omnibus HIPAA Final Rule.

The total estimated annual costs associated with compliance with Privacy Rule information collection requirements have increased from $1,366,679,019 to $1,413,379,050.

Finally, many of the costs for compliance with the applicable requirements of the HIPAA Rules have increased due to an increase in median annual wages for the applicable labor categories, as shown below.

| Occupation | Previous Estimated Wage (including 50% for benefits) | Current Estimated Wage (including 50% for benefits) |
|---|---|---|
| Office and Administrative Support Occupations | $22.53 | $23.46 |
| All Occupations | $24.86 | $25.63 |
| Healthcare Practitioners and Technical Workers | $42.96 | $44.50 |
| Equivalent to GS-12 Level | $43.50 | $44.64 |
| Management Analyst | $56.61 | $58.33 |
| Information Security Analyst | (Not Used) | $64.11 |
| All Management Occupations | $67.00 | $70.12 |
| Public Relations Manager | $67.29 | $73.20 |

**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.