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 extension of a previously approved Office for Civil Rights (OCR) information collection, OMB #0945-0003. There are no program changes associated with this revision. Specifically, we request approval to update certain estimates for the information collection 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 Act (HITECH),[2] the Genetic Information Nondiscrimination Act (GINA),[3] and their implementing regulations at 45 CFR Parts 160 and 164--the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules--establish requirements for covered entities (health plans, health care clearinghouses, and most health care providers) and their business associates with respect to individuals' protected health information (PHI). The information collections in the HIPAA Rules include requirements for recordkeeping, reporting, and third-party disclosures.

[1] Public Law 104-191 (42 U.S.C. 1320d-2(note)).
[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).
[3] Public Law 110-233.

2. Purpose and Use of Information Collection

The HIPAA Privacy Rule contains requirements related to the use, disclosure, and safeguarding of PHI by covered entities and, to some extent, their business associates. The Privacy Rule also ensures that individuals are able to exercise certain rights with respect to their PHI, including the rights to access and seek amendments to their health records and to receive a Notice of Privacy Practices (NPP) from their direct treatment providers and health plans. Accordingly, covered entities are required to provide certain information to individuals, and to produce documentation showing that they have established and implemented policies and procedures to fulfill the Privacy Rule's requirements when asked by OCR for purposes of determining compliance.

The HIPAA Security Rule requires that covered entities and business associates maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI; protect against any reasonably anticipated threats or hazards to the security of the PHI; and prevent reasonably anticipated impermissible uses or disclosures. Covered entities and business associates are required to produce documentation to demonstrate their implementation of reasonable and appropriate safeguards when asked by OCR for purposes of determining compliance.

The HIPAA Breach Notification Rule requires covered entities to provide notification of a breach of unsecured PHI to the Secretary of HHS; affected individuals to alert them that their PHI has been compromised and to encourage them to take the necessary steps to prevent any resulting harm; and, in situations in which a breach affects more than 500 residents of a state or jurisdiction, a prominent media outlet serving that State or jurisdiction. Covered entities are

required to produce documentation to demonstrate their compliance with the breach notification provisions when asked by OCR for purposes of determining compliance.

Without these information collection requirements, OCR would be unable to enforce compliance with the HIPAA Rules, and individuals would be unable to exercise their rights with respect to their PHI or receive notification when their PHI is breached.

3. Use of Improved Information Technology and Burden Reduction

The HIPAA Rules were designed to allow covered entities at different levels of technological sophistication to comply with the requirements of the regulations. Thus, covered entities are empowered to determine appropriate technologies for their circumstances 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 PHI electronically and generally are required to provide individuals with access to their PHI in electronic form if requested by the individual.

The Security Rule applies to entities that create, receive, maintain or transmit electronic PHI. 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 means 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 (*i.e.*, when they have insufficient or out-of-date contact information for individuals) have the option of providing this notification electronically on the home page of their website. 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 PHI are consistent with certain other security frameworks and requirements, such as those provided by the National Institute for Standards and Technology (NIST), which apply to Federal government entities (including some covered entities). 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 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 PHI as defined by HIPAA. Even in cases where a breach of PHI would trigger notification under both state law and HIPAA, 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 reasonable and appropriate methods for compliance depending on the size, capabilities, practices, and security risks of each covered entity and business associate.

With regard to the HIPAA Breach Notification Rule, the burden upon covered entities and business associates of any size to provide the appropriate notifications occurs only when there has been a breach of unsecured PHI. Covered entities and business associates have no obligations under the Breach Notification Rule in the absence of a breach. Further, covered entities and business associates can prevent many breaches, and thus avoid the resulting Breach Notification obligations, by implementing reasonable and appropriate protections for PHI 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 health care activities by HIPAA covered entities and business associates involving PHI, 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. The Breach Notification Rule implements the HITECH Act's requirements for business associates to notify covered entities following the discovery of a breach of PHI, and for covered entities to provide notification to individuals following every breach of unsecured PHI, media notification following every breach affecting more than 500 residents of a state or jurisdiction, and notification to the Secretary of HHS following every breach (within 60 days after discovery for breaches affecting 500 or more individuals and annually for those affecting less than 500). The statute provides no opportunity to provide the required notifications 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 July 19, 2019 (84 FR 34905). No public comments were received.

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 PHI affecting 500 or more individuals, OCR does not provide assurance of confidentiality to the covered entities and business associates involved because the HITECH Act requires this information to be posted on the HHS website 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 burden hours for respondents to comply with the information collection requirements of the HIPAA Privacy, Security, and Breach Notification Rules is 921,158,941 burden hours at a cost of $66,812,896,049. Details are presented below.

12A. Estimated Annualized Burden Hours

For ease of reference, footnotes attached to the table below indicate how we calculated estimates, although the formulas and assumptions behind many of the estimates remain unchanged since the previously approved information collection.[4] 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' compliance activities, or who make use of a provision to exercise an individual right

[4] *See* https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201710-0945-002.

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	Total Responses	Average Burden hours per Response[5]	Total Burden Hours
160.204	Process for Requesting Exception Determinations (states or persons)	1	1	1	16	16
164.308	Risk Analysis - Documentation	1,700,000[6]	1	1,700,000	10	17,000,000
164.308	Information System Activity Review – Documentation	1,700,000	12	20,400,000	.75	15,300,000
164.308	Security Reminders – Periodic Updates	1,700,000	12	20,400,000	1	20,400,000
164.308	Security Incidents (other than breaches) – Documentation	1,700,000	52	88,400,000	5	442,000,000
164.308	Contingency Plan – Testing and Revision	1,700,000	1	1,700,000	8	13,600,000
164.308	Contingency Plan – Criticality Analysis	1,700,000	1	1,700,000	4	6,800,000

[5] 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 due to their size and complexity.

[6] 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.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.310	Maintenance Records	1,700,000	12	20,400,000	6	122,400,000
164.314	Security Incidents – Business Associate reporting of incidents (other than breach) to Covered Entities	1,000,000	12	12,000,000	20	240,000,000
164.316	Documentation – Review and Update[7]	1,700,000	1	1,700,000	6	10,200,000
164.404	Individual Notice—Written and E-mail Notice (drafting)	58,482[8]	1	58,482	.5	29,241
164.404	Individual Notice—Written and E-mail Notice (preparing and documenting notification)	58,482	1	58,482	.5	29,241
164.404	Individual Notice—Written and E-mail Notice (processing and sending)	58,482	1,941[9]	113,513,562	.008	908,108
164.404	Individual Notice—Substitute Notice	2,746[10]	1	2,746	1	2,746

[7] 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.

[8] Total number of breach reports submitted to OCR in 2015. Breaches reported to OCR in 2015 affected more individuals than have been affected by breaches reported in each subsequent year; therefore, we base our burden estimates on 2015 data to ensure that we fully account for the annual burdens of the Breach Notification Rule.

[9] Average number of individuals affected per breach incident reported in 2015.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	(posting or publishing)					
164.404	Individual Notice—Substitute Notice (staffing toll-free number)	2,746	1	2,746	3.42[11]	9,391
164.404	Individual Notice—Substitute Notice (individuals' voluntary burden to call toll-free number for information)	113,264[12]	1	113,264	.125[13]	14,158
164.406	Media Notice	267[14]	1	267	1.25	334
164.408	Notice to Secretary (notice for breaches affecting 500 or more individuals)	267	1	267	1.25	334
164.408	Notice to Secretary	58,215[15]	1	58,215	1	58,215

[10] This number includes all 267 large breaches and all 2,479 breaches affecting 10-499 individuals that were reported to OCR in 2015. 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.

[11] This assumes that 10% of the sum of (a) all individuals affected by large breaches in 2015 (113,250,136) and (b) 5% of individuals affected by small breaches (0.05 x 285,413 = 14,271) will require substitute notification. Thus, we calculate 0.10 x (113,250,136 + 14,271) = 11,326,441 affected individuals requiring substitute notification for an average of 4,125 affected individuals per such breach. We assume that 1% of the affected individuals per breach requiring substitute notice annually will follow up with a telephone call, resulting in 41.25 individuals per breach calling the toll-free number. We assume that call center staff will spend 5 minutes per call, with an average of 41 affected individuals per breach requiring substitute notice, resulting in 3.42 hours per breach spent answering calls from affected individuals.

[12] As noted in the previous footnote, this number equals 1% of the affected individuals who require substitute notification (0.01 x 11,326,441).

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

[14] The total number of breaches affecting 500 or more individuals for which OCR received reports in 2015.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	(notice for breaches affecting fewer than 500 individuals)					
164.410	Business Associate notice to Covered Entity - 500 or more individuals affected	20	1	20	50	1,000
164.410	Business Associate notice to Covered Entity – Less than 500 individuals affected	1,165	1	1,165	8	9,320
164.414	500 or More Affected Individuals (investigating and documenting breach)	267	1	267	50	13,350
164.414	Less than 500 Affected Individuals (investigating and documenting breach)	2,479 (breaches affecting 10-499 individuals)	1	2,479	8	19,832
		55,736 (breaches affecting <10 individuals)	1	55,736	4	222,944
164.504	Uses and Disclosures –	700,000	1	700,000	0.083333333	58,333

[15] The total number of breaches affecting fewer than 500 individuals for which OCR received reports in 2015.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	Organizational Requirements					
164.508	Uses and Disclosures for Which Individual authorization is required	700,000	1	700,000	1	700,000
164.512	Uses and Disclosures for Research Purposes	113,524[16]	1	113,524	0.083333333	9,460
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by paper mail)	100,000,000[17]	1	100,000,000	0.004166667 [1 hour per 240 notices]	416,667
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by electronic mail)	100,000,000	1	100,000,000	0.002783333 [1 hour per 360 notices]	278,333

[16] The number of entities who use and disclose protected health information for research purposes.

[17] 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.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.520	Notice of Privacy Practices for Protected Health Information (health care providers – dissemination and acknowledgement)	613,000,000[18]	1	613,000,000	0.05	30,650,000
164.522	Rights to Request Privacy Protection for Protected Health Information	20,000[19]	1	20,000	0.05	1,000
164.524	Access of Individuals to Protected Health Information (disclosures)	200,000[20]	1	200,000	0.05	10,000
164.526	Amendment of Protected Health Information (requests)	150,000	1	150,000	0.083333333	12,500
164.526	Amendment of Protected Health Information (denials)	50,000	1	50,000	0.083333333	4,167
164.528	Accounting for Disclosures of	5,000[21]	1	5,000	0.05	250

[18] 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.
[19] We assume covered entities address 20,000 requests for confidential communications or restrictions on disclosures per year.
[20] We estimate that covered entities annually fulfill 200,000 requests from individuals for access to their protected health information.
[21] We estimate that covered entities annually fulfill 5,000 requests from individuals for an accounting of disclosures of their protected health information.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	Protected Health Information					
Total				**1,097,206,223**		**921,158,940**

12B. Estimated Annualized Burden Costs

The total cost of this information collection, apart from capital costs, is approximately $66,812,896,049.

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	$59.13[22]	$946
164.308	Risk Analysis - Documentation	17,000,000	$73.89[23]	$1,256,130,000
164.308	Information System Activity Review – Documentation	15,300,000	$73.89	$1,130,517,000
164.308	Security Reminders – Periodic Updates	20,400,000	$73.89	$1,507,356,000
164.308	Security Incidents (other than breaches) – Documentation	442,000,000	$73.89	$32,659,380,000
164.308	Contingency Plan – Testing and Revision	13,600,000	$73.89	$1,004,904,000
164.308	Contingency Plan – Criticality Analysis	6,800,000	$73.89	$502,452,000
164.310	Maintenance Records	122,400,000	$68.07[24]	$8,331,768,000
164.314	Security Incidents – Business Associate reporting of incidents (other than breach) to Covered Entities	240,000,000	$73.89	$17,733,600,000
164.316	Documentation – Review and Update	10,200,000	$73.89	$753,678,000
164.404	Individual Notice— Written and E-mail Notice (drafting)	29,241	$59.13	$1,729,020
164.404	Individual Notice—	29,241	$28.13[25]	$822,403

[22] The $59.13 wage, which includes $39.42 plus 50% for benefits, applies to the category "Healthcare Practitioners and Technical Workers."
[23] The $73.89 wage, which includes $49.26 plus 50% for benefits, applies to the category "Information Security Analysts."
[24] The $68.07 wage, which includes $45.38 plus 50% for benefits, applies to "Management Analysts."

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
	Written and E-mail Notice (preparing and documenting notification)			
164.404	Individual Notice—Written and E-mail Notice (processing and sending)	908,108	$28.13	$25,540,551
164.404	Individual Notice—Substitute Notice (posting or publishing)	2,746	$94.89[26]	$260,568
164.404	Individual Notice—Substitute Notice (staffing toll-free number)	9,391	$28.13	$264,131
164.404	Individual Notice—Substitute Notice (individuals burden to call toll-free number for information)	14,158	$37.47[27]	$530,500
164.406	Media Notice	334	$55.80[28]	$18,624
164.408	Notice to Secretary (notice for breaches affecting 500 or more individuals)	334	$55.80	$18,624
164.408	Notice to Secretary (notice for breaches affecting fewer than 500 individuals)	58,215	$28.13	$1,637,297
164.410	Business Associate notice to Covered Entity - 500 or more individuals affected	1,000	$87.66[29]	$87,660
164.410	Business Associate notice to Covered Entity – Less than 500 individuals affected	9,320	$87.66	816,991
164.414	500 or More Affected	13,350	$87.66	$1,170,261

[25] The $28.13wage, including $18.75 plus 50% for benefits, applies to "Office and Administrative Support Occupations."
[26] The $94.89 wage, including $63.26 plus 50% for benefits, applies to "Public Relations Managers."
[27] The $37.47 wage, including $24.98 plus 50% for benefits, is the median wage for "All Occupations."
[28] The $55.80 average cost per hour is derived by calculating the cost for 267 hours for a GS-12 equivalent ($46.35 wage, including $30.90 plus 50% for benefits) and 66 hours for a Public Relations Manager ($94.89 per hour).
[29] The $87.66 wage, including $58.44 plus 50% for benefits, applies to "Management Occupations."

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
	Individuals (investigating and documenting breach)			
164.414	Less than 500 Affected Individuals (investigating and documenting breach)	19,832 (for breaches affecting 10-499	$87.66	$1,738,473
		222,944 (for breaches affecting <10 individuals)	$87.66	$19,543,271
164.504	Uses and Disclosures – Organizational Requirements	58,333	$59.13	$3,449,250
164.508	Uses and Disclosures for Which Individual authorization is required	700,000	$59.13	$41,391,000
164.512	Uses and Disclosures for Research Purposes	9,460	$59.13	$559,390
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by paper mail)	416,667	$28.13	$11,718,750
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by electronic mail)	278,333	28.13	$7,828,125
164.520	Notice of Privacy Practices for Protected Health Information (health care providers – dissemination and acknowledgement)	30,650,000	$59.13	$1,812,334,500
164.522	Rights to Request Privacy Protection for Protected Health Information	1,000	$59.13	$59,130
164.524	Access of Individuals to Protected Health Information (disclosures)	10,000	$59.13	$591,300
164.526	Amendment of Protected	12,500	$59.13	$739,125

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
	Health Information (requests)			
164.526	Amendment of Protected Health Information (denials)	4,167	$59.13	$246,375
164.528	Accounting for Disclosures of Protected Health Information	250	$59.13	$14,783
Total				**$66,812,896,049**

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

The total capital cost for covered entities and business associates is $118,027,545. The capital cost for providing the required breach notifications is $40,787,745. Capital costs of $77,239,800 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	$671[30]	$39,265,263
164.404	Individual Notice—Substitute Notice Media Posting	2,746[31]	$480	$1,318,080
164.404	Individual Notice—Substitute Notice—Toll-Free Number	2,746	$74.44[32]	$204,403
Section	**Cost Elements**	**Number of Notices of Privacy Practices (NPP)**	**Average Cost per NPP**	**Total NPP Costs**
164.520	Printing for Notice of Privacy Practices for Protected Health Information (health plans)	100,000,000	$.10	$10,000,000[33]
164.520	Postage and Envelope for Notice of Privacy Practices for Protected Health Information (health plans)	10,000,000	$.59	$5,939,800[34]
164.520	Printing Notice of Privacy Practices for Protected Health Information (health care providers)	613,000,000	$.10	$61,300,000[35]
Total				**$118,027,545**

14. Annualized Cost to Federal Government

[30] We again assume that half of all affected individuals (half of 113,535,549 equals 56,767,775) would receive paper notification and half would receive notification by email. Therefore, on average, 971 individuals per breach will receive notification by mail. Further, we estimate that each mailed notice will cost $.06 for paper and envelope, $.08 for printing, and $.55 for postage. Accordingly, on average, the capital cost for mailed notices for each breach is $.69 for each of 971 notices, or $671.41.

[31] The number of breaches requiring substitute notice equals all 267 large breaches and all 2,479 breaches affecting 10-499 individuals.

[32] This number includes $60 per breach for start-up and monthly costs, plus $.35 cents per call (at a standard rate of $.07 per minute for five minutes) for an average of 41.25 individual calls per breach.

[33] This number is based on the assumption that each of 100 million paper notices costs $.10 to print ($.02 per sheet of paper plus $.08 for printing), for a total of $10 million in printing costs.

[34] This number results from the following assumptions: 10% of 100 million notices (10,000,000) will be mailed separately from regular health plan mailings; and each separately mailed paper notice costs $.59 ($.04 for envelope plus $.55 for postage), for a total of $5.9 million in mailing costs.

[35] This estimate includes 613 million notices with a combined cost for paper and printing of $.10 per notice.

The HIPAA Privacy and Security Rules require covered entities and business associates to collect, maintain, and disclose information to comply with the Rules' requirements. However, OCR does not produce the forms on which the information is collected, OCR generally does not collect and store this information, nor does OCR require covered entities and business associates to provide OCR with all information they collect, maintain, or transmit to comply with the Rules. (The one exception to this general rule is that OCR collects documentation from regulated entities in the course of investigations, compliance reviews, and audits to determine compliance 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 associates with the required notifications 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 website a list of the covered entities that have experienced breaches affecting 500 or more individuals. The initial posting of such breaches is automated and OCR pays a contractor approximately $13,000 annually to maintain the database to receive reports of breaches from covered entities. Additionally, OCR drafts and posts summaries of each large breach on the website at a labor cost of approximately $22,600 per year. Therefore, the annualized cost to the federal government is approximately $35,600.

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. We have adjusted the estimated annual burdens of compliance to (1) correct a rounding error; (2) correct an error in the 2016 ICR that underestimated the average number of individuals affected per breach incident because it relied on older breach data, and thus have increased the estimate from 353 individuals to 1,941 individuals per breach; (3) lower the estimated number of individuals who call an entity's toll-free number for information after being affected by a breach requiring substitute notice to reflect a more realistic estimate about the proportion of individuals who choose to call; (4) recognize for the first time the burdens resulting from the pre-existing, ongoing requirement for business associates to report breaches of PHI to their covered entities; and (5) for estimated costs associated with burden hours, reflect increases in average wages using 2018 BLS data for the applicable labor categories. The changes to estimated burden hours are shown in the table below.

Changes to Hourly Burden Estimates from Previously Approved Information Collection

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Burden Hours Per Response	Total Burden Hours	Reason for Modification
164.404	Individual Notice—Written and E-mail Notice (drafting)	Previously Approved: 58,481 Modified: 58,482 **Increase of 1**	1	Previously Approved: 58,481 Modified: 58,482 **Increase of 1**	.5	Previously Approved: 29,240 Modified: 29,241 **Increase of 1**	Changes due to rounding.
164.404	Individual Notice—Written and E-mail Notice (preparing and documenting notification)	Previously Approved: 58,481 Modified: 58,482 **Increase of 1**	1	Previously Approved: 58,481 Modified: 58,482 **Increase of 1**	.5	Previously Approved: 29,240 Modified: 29,241 **Increase of 1**	Changes due to rounding.
164.404	Individual Notice—Written and E-mail Notice (processing and sending)	Previously Approved: 58,481 Modified: 58,482 **Increase of 1**	Previously Approved: 353 Modified: 1,948 **Increase of 1,595**	Previously Approved: 20,643,793 Modified: 113,513,562 **Increase of 92,869,769**	.008	Previously Approved: 165,150 Modified: 908,108 **Increase of 742,958**	Changes due to rounding and corrected (updated) breach data.
164.404	Individual Notice—Substitute Notice (staffing toll-free number)	2,746	1	2,746	Previously Approved: 5.75 Modified: 3.42 **Decrease of 2.33**	Previously Approved: 15,789 Modified: 9,391 **Decrease of 6,398**	Changes due to corrected (updated) breach data.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Burden Hours Per Response	Total Burden Hours	Reason for Modification
164.404	Individual Notice—Substitute Notice (individuals' voluntary burden to call toll-free number for information)	Previously Approved: 11,326,440 Modified: 113,264 **Decrease of 11,213,176**	1	Previously Approved: 11,326,440 Modified: 113,264 **Decrease of 11,213,176**	.125	Previously Approved: 1,415,805 Modified: 14,158 **Decrease of 1,401,647**	Changes due to how OCR is calculating the estimate (lowered estimate of # of individuals who call a toll-free #).
164.406	Media Notice	267	1	267	1.25	Previously Approved: 333 Modified: 334 **Increase of 1**	Change due to rounding.
164.408	Notice to Secretary (notice for breaches affecting 500 or more individuals)	267	1	267	1.25	Previously Approved: 333 Modified: 334 **Increase of 1**	Change due to rounding.
164.410	Business Associate notice to Covered Entity – 500 or more individuals affected	Previously Approved: 0 Modified: 20 **Increase of 20**	Previously Approved: 0 Modified: 1 **Increase of 1**	Previously Approved: 0 Modified: 20 **Increase of 20**	Previously Approved: 0 Modified: 50 **Increase of 50**	Previously Approved: 0 Modified: 1,000 **Increase of 1,000**	Recognize for the first time the burdens resulting from the pre-existing, ongoing requirement for business associates to report breaches of PHI to their covered entities.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Burden Hours Per Response	Total Burden Hours	Reason for Modification
164.410	Business Associate notice to Covered Entity – Less than 500 individuals affected	Previously Approved: 0 Modified: 1,165 **Increase of 1,165**	Previously Approved: 0 Modified: 1 **Increase of 1**	Previously Approved: 0 Modified: 1,165 **Increase of 1,165**	Previously Approved: 0 Modified: 8 **Increase of 8**	Previously Approved: 0 Modified: 9,320 **Increase of 9,320**	Recognize for the first time the burdens resulting from the pre-existing, ongoing requirement for business associates to report breaches of PHI to their covered entities.
164.526	Amendment of Protected Health Information (denials)	50,000	1	50,000	0.05	Previously Approved: 4,166 Modified: 4,167 **Increase of 1**	Change due to rounding.
Previously Approved Total Number of Responses and Burden Hours For the Collections in this Table				**32,089,941**		**1,655,224**	
Modified Total Number of Responses and Burden Hours For the Collections in this Table				**113,747,721**		**1,000,462**	
Changes to Total Number of Responses and Burden Hours				**+ 81,657,780**		**- 654,762**	
Previously Approved Total Number of Responses and Burden Hours for the Entire ICR				**1,015,548,443**		**921,813,702**	

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Burden Hours Per Response	Total Burden Hours	Reason for Modification
Modified Total Number of Responses and Burden Hours for the Entire ICR				**1,097,206,223**		**921,158,940**	

As a result, the total estimated annual labor and capital costs associated with compliance with the HIPAA Rules' information collections, apart from costs to the Federal government, have increased from $57,791,284,929 to $66,930,923,594.

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.