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

The Office for Civil Rights (OCR) at the U.S. Department of Health & Human Services (HHS) is requesting OMB approval for the revision of a previously approved OCR information collection, OMB #0945-0003. There are significant program changes associated with this revision as detailed in the Notice of Proposed Rulemaking (NPRM) on Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement.[1] As a result of these proposed changes, OCR requests approval to update, adjust, and add 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),[2] the Health Information Technology for Economic and Clinical Health Act (HITECH),[3] the Genetic Information Nondiscrimination Act (GINA),[4] 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

[1] 86 FR 6446 (January 21, 2021).
[2] Public Law 104-191 (42 U.S.C. 1320d-2(note)).
[3] 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).
[4] Public Law 110-233.

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.

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; to 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, to 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 requirements under both state law and HIPAA, OCR believes 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

The proposed changes to the HIPAA Privacy Rule, would result in a need for covered entities to perform some one-time information collection activities, such as revising and establishing policies and procedures, updating workforce training content, and posting new or updated documents online.

The frequency of the ongoing information collection requirements 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 proposed rule was published for public comment under Regulation Identifier Number (RIN) 0945-AA00, 86 FR 6446 (January 21, 2021).

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 (5 USC 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, including one-time burdens presented by proposed program changes is 952,089,673 burden hours at a cost of $93,937,597,924. Details are presented below.

12A. Estimated Annualized Burden Hours

Due to the number of proposed changes to the Privacy Rule that would affect the information collection, OCR presents in separate tables the collections that would be unaffected by NPRM's proposals, new ongoing burdens, new one-time burdens, and adjustments due to previously unacknowledged burdens. For ease of reference, footnotes attached to the table below indicate how OCR calculated estimates, although the formulas and assumptions behind many of the estimates for the Security and Breach Notification Rules remain unchanged since the previously approved information collection.[5] Consistent with OCR's previous regulatory ICRs, this ICR sometimes counts 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 under the Rules. Although OCR believes this makes the calculations more transparent, it is not always obvious for any given provision which individuals or entities constitute the "respondents," so OCR states the types of respondents 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 OCR indicates 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

[5] *See* https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201909-0945-001.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden Hours per Response	Total Burden Hours
160.204	Process for Requesting Exception Determinations — states or persons	1	1	1	16[6]	16
164.308	Contingency Plan—Testing and Revision	1,774,331	1	1,774,331	8	14,194,648
164.308	Contingency Plan—Criticality Analysis	1,774,331	1	1,774,331	4	7,097,324
164.310	Maintenance Records	1,774,331	12	21,291,972	6	127,751,832
164.314	Security Incidents – Business Associate reporting of non-breach incidents to Covered Entities	1,000,000	12	12,000,000	20	240,000,000
164.316	Risk Analysis—Documentation, 164.308	1,774,331[7]	1	1,774,331	10[8]	17,743,310
164.316	Information System Activity Review—Documentation, 164.308	1,774,331	12	21,291,972	.75	15,968,979
164.316	Security Reminders—Periodic Updates, 164.308	1,774,331	12	21,291,972	1	21,291,972

[6] 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.

[7] This estimate includes 774,331 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, the Department believes the lower end of this range is more accurate.

[8] 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.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden Hours per Response	Total Burden Hours
164.316	Security Incidents—Other than breaches—Documentation, 164.308	1,774,331	52	92,265,212	5	461,326,060
164.316	Documentation—Review and Update, 164.306	1,774,331	1	1,774,331	6	10,645,986
164.404	Individual Notice—Written and E-mail Notice—Drafting	58,482[9]	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[10]	113,513,562	.008	908,108
164.404	Individual Notice—Substitute Notice—Posting or publishing	2,746[11]	1	2,746	1	2,746
164.404	Individual	2,746	1	2,746	3.42[12]	9,391

[9] 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, the Department bases its burden estimates on 2015 data to ensure that it fully accounts for the annual burdens of the Breach Notification Rule.

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

[11] This number includes all 267 large breaches and all 2,479 breaches affecting 10-499 individuals that were reported to OCR in 2015. As the Department stated in the preamble to the Omnibus HIPAA Final Rule, although some breaches involving fewer than 10 individuals may require substitute notice, it believes the costs of providing such notice through alternative written means or by telephone is negligible.

[12] 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, the Department calculates 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. The Department assumes that 1% of the affected individuals per breach requiring substitute notice annually will follow up with a telephone call, resulting in

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden Hours per Response	Total Burden Hours
	Notice—Substitute Notice—Staffing toll-free number					
164.404	Individual Notice—Substitute Notice—Individuals' voluntary burden to call toll-free number for information	113,264[13]	1	113,264	.125[14]	14,158
164.406	Media Notice	267[15]	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—Notice for breaches affecting fewer than 500 individuals	58,215[16]	1	58,215	1	58,215
164.410	Business Associate notice to Covered Entity—500 or more individuals affected	20	1	20	50	1,000
164.410	Business Associate	1,165	1	1,165	8	9,320

41.25 individuals per breach calling the toll-free number. The Department assumes 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.

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

[14] 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.

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

[16] 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
	notice to Covered Entity— Less than 500 individuals affected					
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 – Organizational Requirements	774,331	1	774,331	0.083333333	64,528
164.508	Uses and Disclosures for Which Individual Authorization is Required	774,331	1	774,331	1	774,331
164.512	Uses and Disclosures for Research Purposes	113,524[17]	1	113,524	0.08333333	9,460
164.520	Notice of Privacy Practices for Protected Health Information—Health plans —Periodic	100,000,000[18]	1	100,000,000	0.00416666 [1 hour per 240 notices]	416,667

[17] The number of entities who use and disclose PHI for research purposes.

[18] As in the Department's previous submission, it assumes 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
	distribution of NPPs by paper mail					
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	0.00278333 [1 hour per 360 notices]	278,333
164.520	Notice of Privacy Practices for Protected Health Information—Health care providers—Dissemination	613,000,00[19]	1	613,000,000	0.02083333[20]	12,770,833
164.522	Rights to Request Privacy Protection for Protected Health Information	40,000[21]	1	40,000	0.05	2,000
164.524	Access of Individuals to Protected Health Information—Copies of PHI	1,230,000[22]	1	1,230,000	0.01666667[23]	20,500
164.526	Amendment of Protected Health	150,000	1	150,000	0.08333333	12,500

[19] The Department estimates that each year covered health care providers will have first-time visits with 613 million individuals, to whom the providers must give an NPP.
[20] This represents 1 minute and fifteen seconds (75/3,600) to disseminate the NPP and eliminates the 1 minute and 45 seconds previously allocated for obtaining the signed patient acknowledgement.
[21] The Department doubled the estimated number of requests for confidential communications or restrictions on disclosures per year due to the combined effect of changes to the minimum necessary standard and the information blocking provisions of the ONC Cures Act Final Rule.
[22] The Department has increased its estimate of the number of requests from individuals for copies of their PHI that covered entities annually provide to them directly to 1,230,000.
[23] This represents an estimated average of 1 minute per request which is not chargeable as a fee to the individual.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden Hours per Response	Total Burden Hours
	Information—Requests					
164.526	Amendment of Protected Health Information—Denials	50,000	1	50,000	0.08333333	4,167
164.528	Accounting for Disclosures of Protected Health Information	5,000[24]	1	5,000	0.05	250
TOTAL						931,691,910

New or Previously Unacknowledged Ongoing Burdens of Compliance, Annualized

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
164.514	Minimum necessary evaluations for treatment, payment, and health care operations—Uses and disclosures	774,331	1	774,331	14[25]	10,840,634[26]

[24] The Department estimates that covered entities annually fulfill 5,000 requests from individuals for an accounting of disclosures of their PHI.

[25] 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.

[26] This represents a previously unacknowledged annual burden of 18 hours per covered entity for making minimum necessary evaluations for purposes of treatment, payment, and health care operations uses and disclosures, reduced by an estimated 4 burden hours annually per covered entity (or 3,097,324 total) as a result of the proposed changes to the minimum necessary standard combined with proposed changes to the definition of health care operations.

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 — Right to discuss privacy practices	6,130,000	1	6,130,000[27]	0.1166667	715,167
164.524	Access of Individuals to Protected Health Information —Provider submitting individual's access request to another provider or plan	92,250	1	92,250[28]	.0583333[29]	5,381
164.524	Access of Individuals to Protected Health Information —Directing copies of ePHI to health plans and providers	153,750[30]	1	153,750	0.0666666	10,250
164.524	Access of Individuals to Protected Health Information	153,750[31]	1	153,750	0.0333333	5,125

[27] 1% of an estimated 613 million new patient encounters annually.
[28] 15% of 615,000 annual access requests to direct electronic copies of ePHI to health plans and providers as third parties under the right of access.
[29] This represents 3.5 minutes for a medical assistant to obtain the needed information and submit it for the individual.
[30] This represents one-fourth of the estimated 615,000 annual requests under the right of access for copies of ePHI directed to health plans and health care providers as third parties and reflects only the labor burden for such requests for ePHI to be sent via other than an internet-based method (e.g., on electronic media and mailed to the recipient).
[31] This represents one-fourth of the estimated 615,000 annual requests for copies of ePHI directed to third parties and reflects only uncompensated the labor burden for requests for ePHI to be sent via other than an internet-based method (e.g., on electronic media and mailed to the recipient).

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	—Directing copies of ePHI to third parties other than health plans and providers					
164.525	Notice of Access and Authorization Fees—Individualized estimates	73,800	1	73,800[32]	0.05	3,690
164.525	Notice of Access and Authorization Fees—Item-ized list of charges for copies	24,600[33]	1	24,600	0.0166667	410
TOTAL						**11,580,657**

New One-time Burdens of Compliance

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	774,331	1	774,331	0.16666667[34]	129,055

[32] 3% of an estimated 2.46 million annual access requests for copies of PHI.
[33] 1% of an estimated 2.46 million annual access requests for copies of PHI.
[34] 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.

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—Post updated notice online					
164.525	Notice of Fees for Copies of PHI—Post fee schedule online	774,331	1	774,331	.1666667	129,055
164.530	Administrative Requirements—Training Minimum necessary, 164.514	774,331	1	774,331	1	774,331
164.530	Administrative Requirements—Training— Right of access, 164.525, and fee estimates, 164.525—Updated training content	774,331	1	774,331	2.5	1,935,828
164.530	Administrative Requirements—Training—Access—Workforce member time in training, 164.524	774,331	1	774,331	0.116666667	90,339
164.530	Administrative Requirements—Training—Disclosing PHI under164.510; uses and disclosures to prevent harm, 164.512	768,169	1	768,169	0.6666667	512,113
164.530	Administrative Requirements—Training—Disclosures for Uniformed Services, & disclosures to Telecommunications Relay Services for treatment, payment and health care	774,331	1	774,331	0.25	193,583

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	operations, 164.512					
164.530	Administrative Requirements—Training—Notice of privacy practices, changes in content & right to discuss privacy practices, 164.520	774,331	1	774,331	0.0833333	64,528
164.530	Administrative Requirements—Training—Verification of identity, 164.514	38,717[35]	1	38,717	0.1666667	6,453
164.530	Administrative Requirements—Policies & Procedures—Individual care coordination and case management, 164.501 & 164.502, minimum necessary, 164.514, and social services agencies for care coordination, 164.506	774,331	1	774,331	1.25	967,914
164.530	Administrative Requirements—Policies & Procedures—Right of access, 164.524, & fee estimates, 164.525	774,331	1	774,331	3	2,322,993
164.530	Administrative Requirements—Policies & Procedures—Disclosing PHI under 164.510;	768,169[36]	1	768,169	1	768,169

[35] This represents 5% of all covered entities.
[36] This represents all health care providers.

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Total Responses	Average Burden hours per Response	Total Burden Hours
	uses and disclosures to prevent harm, 164.512(j)					
164.530	Administrative Requirements—Policies & Procedures—Revising the Notice of Privacy Practices, 164.520	774,331	1	774,331	1	774,331
164.530	Administrative Requirements—Policies & Procedures—Disclosures for Uniformed Services & Telecommuni-cations Relay Services, 164.512	774,331	1	774,331	0.16666667[37]	129,055
164.530	Administrative Requirements—Polices & Procedures—Identity verification changes, 164.514	38,717[38]	1	38,717	0.5	19,358
TOTAL				10,131,413		**8,817,103[39]**

12B. Estimated Annualized Burden Costs

The total cost of this information collection, apart from capital costs, is approximately $93,913,549,924. These figures are based on annual wage rates. Benefits are calculated by multiplying the base hourly wage rate by two. The labor costs of this information collection

[37] This equates to 10 minutes.
[38] This represents 5 percent of all covered entities.
[39] Total may not add up due to rounding.

reflect a doubling of the costs of benefits from 50% of the base wage to 100% of the base wage as compared to the previous information collections for the HIPAA Rules.

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	$80.42[40]	$1,287
164.308	Risk Analysis - Documentation	17,743,310	$100.20[41]	$1,777,879,662
164.308	Information System Activity Review – Documentation	15,968,979	$100.20	$1,600,091,696
164.308	Security Reminders – Periodic Updates	21,291,972	$100.20	$2,133,455,594
164.308	Security Incidents (other than breaches) – Documentation	461,326,060	$100.20	$46,224,871,212
164.308	Contingency Plan – Testing and Revision	14,194,648	$100.20	$1,422,303,730
164.308	Contingency Plan – Criticality Analysis	7,097,324	$100.20	$533,363,899
164.310	Maintenance Records	127,751,832	$91.88[42]	$11,737,838,324
164.314	Security Incidents – Business Associate reporting of incidents (other than breach) to Covered Entities	240,000,000	$100.20	$24,048,000,000
164.316	Documentation – Review and Update	10,645,986	$100.20	$1,066,727,797
164.404	Individual Notice—Written and E-mail Notice (drafting)	29,241	$80.42	$2,351,561
164.404	Individual Notice—	29,241	$39.46[43]	$1,153,850

[40] The $80.42 wage, which includes $40.21 plus 100% for benefits, applies to the category "Healthcare Practitioners and Technical Workers."
[41] The $100.20 wage, which includes $50.10 plus 100% for benefits, applies to the category "Information Security Analysts."
[42] The $91.88 wage, which includes $45.94 plus 100% for benefits, applies to "Management Analysts."
[43] The $39.46 wage, including $19.73 plus 100% for benefits, applies to "Office and Administrative Support."

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	$39.46	$35,833,961
164.404	Individual Notice—Substitute Notice (posting or publishing)	2,746	$79.20[44]	$217,483
164.404	Individual Notice—Substitute Notice (staffing toll-free number)	9,391	$39.46	$370,581
164.404	Individual Notice—Substitute Notice (individuals burden to call toll-free number for information)	14,158	$51.44[45]	$728,288
164.406	Media Notice	334	$74.61[46]	$24,900
164.408	Notice to Secretary (notice for breaches affecting 500 or more individuals)	334	$74.61	$24,900
164.408	Notice to Secretary (notice for breaches affecting fewer than 500 individuals)	58,215	$39.46	$2,297,164
164.410	Business Associate notice to Covered Entity - 500 or more individuals affected	1,000	$110.74[47]	$110,740
164.410	Business Associate notice to Covered Entity – Less than 500 individuals affected	9,320	$110.74	1,032,097
164.414	500 or More Affected	13,350	$110.74	$1,478,379

[44] The $79.20 wage, including $39.60 plus 100% for benefits, applies to "Web Developers and Digital Interface Designers." Previously, OCR based the wage cost on a Public Relations Managers' hourly rate.
[45] The $51.44 wage, including $25.72 plus 100% for benefits, is the median wage for "All Occupations."
[46] The $74.61 average cost per hour is derived by calculating the cost for 267 hours for a GS-12 equivalent ($61.80 wage, including $30.90 plus 100% for benefits) and 66 hours for a Public Relations Manager ($127.54 per hour) and dividing the sum total by the total number of burden hours.
[47] The $110.74 wage, including $55.37 plus 50% for benefits, applies to "Medical and Health Services Manager."

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	$110.74	$2,196,196
		222,944 (for breaches affecting <10 individuals)	$110.74	$24,688,819
164.504	Uses and Disclosures – Organizational Requirements	64,528	$80.42	$5,189,308
164.508	Uses and Disclosures for Which Individual authorization is required	774,331	$80.42	$62,271,699
164.512	Uses and Disclosures for Research Purposes	9,460	$80.42	$760,800
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by paper mail)	416,667	$39.44	$16,433,333
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by electronic mail)	278,333	39.44	$10,977,467
164.520	Notice of Privacy Practices for Protected Health Information (health care providers – dissemination)	12,770,833	$80.42	$1,027,030,417
164.522	Rights to Request Privacy Protection for Protected Health Information	2,000	$80.42	$160,840
164.524	Access of Individuals to Protected Health Information (disclosing copies of PHI to individuals)	20,500	$44.80	$918,400

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
164.526	Amendment of Protected Health Information (requests)	12,500	$80.42	$1,005,250
164.526	Amendment of Protected Health Information (denials)	4,167	$80.42	$335,083
164.528	Accounting for Disclosures of Protected Health Information	250	$80.42	$20,105
Total				**$91,742,144,820**

New and Previously Unacknowledged Ongoing Annualized Burden Costs

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
164.514	Minimum necessary evaluations for treatment, payment, and health care operations - uses and disclosures	10,840,634	$110.74	$1,200,491,809
164.520	Notice of Privacy Practices for Protected Health Information (right to discuss privacy practices)	715,167	$74.48	$53,265,613
164.524	Access of Individuals to Protected Health Information (disclosing copies of ePHI to health plans and providers)	10,250	$44.80	$459,200
164.524	Access of Individuals to Protected Health Information	5,125	$44.80	$229,600

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
	(disclosing copies of ePHI to other third parties)			
164.524	Access of Individuals to Protected Health Information (submitting requests for individuals to direct copies of ePHI to plans and providers)	5,381	$34.34	$184,792
164.525	Notice of Access and Authorization Fees - Individualized estimates	3,690	$44.80	$165,312
164.525	Notice of Access and Authorization Fees - Itemized list of charges	410	$44.80	$18,368
TOTAL		**11,580,657**		**$1,254,814,695**

One-time Burden Costs

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
164.524	Notice of Privacy Practices for Protected Health Information – Post updated notice online	129,055	$79.20	$10,221,169
164.525	Notice of Fees for Copies of PHI – Post fee schedule online	129,055	$79.20	$10,221,169
164.530	Administrative	774,331	$63.12	$48,875,773

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
	Requirements – Training (minimum necessary, 164.514)			
164.530	Administrative Requirements – Training (right of access and fee estimates)	1,935,828	$63.12	$122,189,432
164.530	Administrative Requirements - Training (right of access and fee estimates - medical records staff)	90,339	$44.80	$4,047,170
164.530	Administrative Requirements – Training (disclosing PHI under 164.510; uses and disclosures to prevent harm, 164.512(j))	512,113	$63.12	$32,324,552
164.530	Administrative Requirements – Training (disclosures for Uniformed Services, 164.512(k); disclosures to Telecommunications Relay Services for treatment, payment and health care operations)	193,583	$63.12	$12,218,943
164.530	Administrative Requirements – Training (notice of privacy practices, changes in content & right to discuss privacy practices, 164.520)	64,528	$63.12	$4,072,981
164.530	Administrative Requirements –	6,453	$63.12	$407,303

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
	Training (verification of identity)			
164.530	Administrative Requirements – Policies & Procedures (minimum necessary and social services agencies for care coordination)	967,914	$139.72[48]	$135,236,909
164.530	Administrative Requirements – Policies & Procedures (right of access & fee estimates)	2,322,993	$139.72	$324,568,582
164.530	Administrative Requirements – Policies & Procedures (disclosures under 164.510; uses and disclosures to prevent harm, 164.512)	768,169	$139.72	$107,328,573
164.530	Administrative Requirements – Policies & Procedures (revising the Notice of Privacy Practices)	774,331	$139.72	$108,189,527
164.530	Administrative Requirements – Policies & Procedures (disclosures for Uniformed Services & Telecommunications Relay Services)	129,055	$139.72	$18,031,588
164.530	Administrative	19,358	$139.72	$2,704,738

[48] The wage rates in the table include the adjusted hourly costs of a lawyer at a cost of $139.72.

Section	Type of Respondent	Total Burden Hours	Hourly Wage Rate	Total Respondent Costs
	Requirements – Policies & Procedures (verification of identity)			
TOTAL		**12,831,010**		**$940,638,409**

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 $118,269,943. 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. In addition, OCR has added capital costs for new requirements to make an access fee schedule available at the point of service, provide individualized estimates of access fees upon request, and provide itemized lists of charges for copies of protected health information upon request, in the total annual amount of $242,398.

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[49]	$39,265,263
164.404	Individual Notice—Substitute Notice Media Posting	2,746[50]	$480	$1,318,080
164.404	Individual Notice—Substitute Notice—Toll-Free Number	2,746	$74.44[51]	$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[52]
164.520	Postage and Envelope for Notice of Privacy Practices for Protected Health Information (health plans)	10,000,000	$.59	$5,939,800[53]
164.520	Printing Notice of Privacy Practices for Protected Health Information (health care providers)	613,000,000	$.10	$61,300,000[54]
Section	**Cost Elements**	**Number of pages**	**Cost per page**	**Total Cost**
164.525	Making fee schedule available at the point of service and upon request.	2,322,993	$.10	$232,299
164.525	Provide an individualized estimate of fees by mail	11,070	$.69	$7,638

[49] OCR again assumes 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, OCR estimates 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.

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

[51] 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.

[52] 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.

[53] 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.

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

Section	Cost Elements	Number of Breaches	Cost per Breach	Total Cost
164.525	Printing itemized list of copy charges	24,600	$.10	$2,460
Total				**$118,269,943**

14. Annualized Cost to Federal Government

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

The NPRM associated with this ICR proposes significant program changes since the previous information collection submission, and thus this information collection reflects new requirements and flexibilities for regulated entities, and modified burdens and benefits for individuals. The Department proposes to modify the Privacy Rule to increase permissible disclosures of PHI and to improve care coordination and case management by:

- Adding definitions for the terms electronic health record (EHR) and personal health application.
- Modifying provisions on the individuals' right of access to PHI by:
    - strengthening individuals' rights to inspect their PHI in person, which includes allowing individuals to take notes or use other personal resources to view and capture images of their PHI;
    - shortening covered entities' required response time to no later than 15 calendar days (from the current 30 days) with the opportunity for an extension of no more than 15 calendar days (from the current 30-day extension);

- clarifying the form and format required for responding to individuals' requests for their PHI;
- requiring covered entities to inform individuals that they retain their right to obtain or direct copies of PHI to a third party when a summary of PHI is offered in lieu of a copy;
- reducing the identity verification burden on individuals exercising their access rights;
- creating a pathway for individuals to direct the sharing of PHI in an EHR among covered health care providers and health plans, by requiring covered health care providers and health plans to submit an individual's access request to another health care provider and to receive back the requested electronic copies of the individual's PHI in an EHR;
- requiring covered health care providers and health plans to respond to certain records requests received from other covered health care providers and health plans when directed by individuals pursuant to the right of access;
- limiting the individual right of access to direct the transmission of PHI to a third party to electronic copies of PHI in an EHR;
- specifying when electronic PHI (ePHI) must be provided to the individual at no charge;
- amending the permissible fee structure for responding to requests to direct records to a third party; and
- requiring covered entities to post estimated fee schedules on their websites for access and for disclosures with an individual's valid authorization and, upon

request, provide individualized estimates of fees for an individual's request for copies of PHI, and itemized bills for completed requests.

- Amending the definition of health care operations to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management that constitute health care operations.
- Creating an exception to the "minimum necessary" standard for individual- level care coordination and case management uses and disclosures. The minimum necessary standard generally requires covered entities to limit uses and disclosures of PHI to the minimum necessary needed to accomplish the purpose of each use or disclosure. This proposal would relieve covered entities of the minimum necessary requirement for uses by, disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management activities with respect to an individual, regardless of whether such activities constitute treatment or health care operations.
- Clarifying the scope of covered entities' abilities to disclose PHI to social services agencies, community-based organizations, home and community based service (HCBS) providers and other similar third parties that provide health-related services, to facilitate coordination of care and case management for individuals.
- Replacing the privacy standard that permits covered entities to make certain uses and disclosures of PHI based on their "professional judgment" with a standard permitting such uses or disclosures based on a covered entity's good faith belief that the use or disclosure is in the best interests of the individual. The proposed standard is more permissive in that it would presume a covered entity's good faith, but this presumption could be overcome with evidence of bad faith.

- Expanding the ability of covered entities to disclose PHI to avert a threat to health or safety when a harm is "serious and reasonably foreseeable," instead of the current stricter standard which requires a "serious and imminent" threat to health or safety.
- Eliminating the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP).
- Modifying the content requirements of the NPP to clarify for individuals their rights with respect to their PHI and how to exercise those rights.
- Expressly permitting disclosures to Telecommunications Relay Services (TRS) communications assistants for persons who are deaf, hard of hearing, or deaf-blind, or who have a speech disability, and modifying the definition of business associate to exclude TRS providers.
- Expanding the Armed Forces permission to use or disclose PHI to all uniformed services, which then would include the U.S. Public Health Service (USPHS) Commissioned Corps and the National Oceanic and Atmospheric Administration (NOAA) Commissioned Corps.

In addition, OCR is making updates and adjustments to certain estimates. OCR has revised the estimated annual burdens of compliance by:

(1) Increasing the number of covered entities from 700,000 to 774,331 due to program change;

(2) Increasing the number of access requests under 45 CFR 164.524 from 200,000 to 2,460,000 annually due to program change;

(3) Increasing the estimated burden hours for responding to access requests under 45 CFR 164.524 from 3 to 5 minutes per request due to program change;

(4) Increasing the burden hours by a factor of two for responding to individuals' requests for restrictions on disclosures of their protected health information under 45 CFR 164.522 due to program change;

(5) Recognizing the burdens resulting from the pre-existing, ongoing requirement for covered entities to make minimum necessary evaluations under 45 CFR 164.514 before using or disclosing protected health information for payment and health care operations purposes (and for using protected health information for treatment) in the amount of 18 hours annually per covered entity, and decrease the annual minimum necessary burden by 4 hours per covered entity due to program change, resulting in a total ongoing annual burden of 14 hours per covered entity;

(6) Recognizing for the first time burdens associated with providing electronic copies of protected health information to third parties designated by individuals under 45 CFR 164.524 in the amount of 2 minutes per request to send electronic copies by other than an internet-based means;

(7) Recognizing for the first time burdens associated with providing electronic copies of protected health information to health plans and health care providers as third parties designated by individuals under 45 CFR 164.524 in the amount of 4 minutes per request to send electronic copies by other than an internet-based means; and

(8) Decreasing the estimated burden for disseminating the Notice of Privacy Practices and obtaining an acknowledgement of receipt under 45 CFR 164.520, from 3 minutes to 1 minute and 15 seconds due to program change.

In addition to these changes, OCR has added new burdens to the ICR as a result of program changes:

(1) An annual burden of 10 minutes per covered entity for posting an updated Notice of Privacy Practices due to program changes;

(2) An annual burden of 3.5 minutes per request for submitting an access request for an individual to another provider for an estimated 92,250 annual requests;

(3) An annual 10-minute burden per covered entity for posting an access and authorization fee schedule online under 45 CFR 164.525;

(4) An annual 7-minute burden for each of an estimated 18,390,000 annual requests from individuals to discuss their direct treating health care provider's Notice of Privacy Practices under 45 CFR 164.520;

(5) An annual three-minute burden for each of an estimated 73,800 annual requests from individuals for an individualized estimate of the fees to provide copies of requested protected health information under 45 CFR 164.525;

(6) An annual one-minute burden for each of an estimated 24,600 annual requests from individuals for an itemized list of charges for their requested copies of protected health information under 45 CFR 164.525;

(7) A one-time burden of 6 hours and 55 minutes for each covered entity to update its policies and procedures under 45 CFR 164.530 due to program changes; and

(8) A one-time burden of 4 hours and 40 minutes for each covered entity to update the content of its HIPAA training program under 45 CFR 164.530 and a related one-time burden of 7 additional minutes of staff time spent in training on 45 CFR 164.524 per covered entity.

-

As a result, the total estimated annual labor and capital costs associated with compliance with the HIPAA Rules' information collections (including one-time costs), apart from costs to the Federal government, have increased from $66,930,923,594 to $94,055,867,867.

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.