**Supporting Statement for**

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

## A. Justification

### 1. Circumstances Making the Collection of Information Necessary

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is requesting OMB approval for the revision of a previously approved OCR information collection, OMB #0945-0003.[1] This information collection addresses requirements under the Health Insurance Portability and Accountability Act (HIPAA) of 1996,[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. These regulations, known as the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (collectively, "HIPAA 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) and rights for individuals with respect to their PHI. The information collections in the HIPAA Rules include requirements for recordkeeping, reporting, and third-party disclosures.

The Department is finalizing modifications to the Privacy Rule. The final rule modifies existing standards permitting uses and disclosures of PHI by limiting uses and disclosures of PHI for certain purposes where the use or disclosure involves reproductive health care that is lawful under the circumstances in which such health care is provided. The final rule prohibits uses and

[1] ICR ref. no. 202211-0945-003.
[2] Pub. L. 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) (Pub. L. 111–5).
[4] Pub. L. 110-233.

disclosures of PHI to investigate or impose liability on individuals, covered entities or their business associates (collectively, "regulated entities"), or other persons for the mere act of seeking, obtaining, providing, or facilitating reproductive health care that is lawful under the circumstances in which such health care is provided, or to identify any person to investigate or impose liability on them for such purposes. This final rule also makes certain modifications to the Privacy Rule's requirements for Notices of Privacy Practices to implement requirements of section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[5]

As a result of updated statistics for covered entities, breaches of PHI, and regulatory modifications, OCR requests approval to update and add certain estimates for the information collection burdens associated with the HIPAA Rules.

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

The 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 demonstrating that they have established and implemented policies and procedures to fulfill the Privacy Rule's requirements when requested by OCR for purposes of determining compliance.

[5] Pub. L. 116–136, 134 Stat. 281 (March 27, 2020).

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

The Breach Notification Rule requires regulated entities to provide notification of a breach of unsecured PHI. A covered entity must notify 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 a prominent media outlet serving that State or jurisdiction in situations in which a breach affects more than 500 residents of a state or jurisdiction. In addition, a business associate must notify the covered entity of a breach of the covered entity's PHI. Regulated entities are required to produce documentation to demonstrate their compliance with the applicable breach notification provisions when asked by OCR for purposes of determining compliance.

Without these information collection requirements, OCR would be unable to investigate and determine 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 regulated 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 covered entities to provide the required NPP 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 regulated entities with respect to the ePHI of a covered entity. Regulated entities that are subject to the Security Rule's requirements are permitted to maintain the required documentation in electronic or paper form.

The 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**

Generally, the information collection requirements of the Privacy and Security Rules do not duplicate those of any other Federal regulation. An unknown number of covered entities that also meet the definition of "Part 2 program" at 42 CFR 2.11 are subject to restrictions on the use and disclosure of substance use disorder (SUD) patient records under 42 U.S.C. 290dd-2. These requirements include providing a patient confidentiality notice to patients who are the subject of records protected by 42 CFR part 2 ("Part 2"). However, the Department does not believe this requirement to be duplicative of the NPP requirements of the Privacy Rule because these entities could meet both HIPAA and Part 2 requirements with a single NPP document, and changes in this final rule facilitate that ability. [6]

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 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

[6] *See* sec. 3221(i), Pub.L.116-136 (March 27, 2020) requiring the Department to modify the HIPAA NPP provision at 45 CFR 164.520 to give notice to individuals of the protections afforded to certain SUD treatment records held by a covered entity.

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, the Department believes that both the state law notification and the notification under this rule can be satisfied with a single breach notification. In addition, breach notification requirements under Part 2 apply the Breach Notification Rule's requirements to breaches of Part 2 records but do not create new obligations for HIPAA regulated entities that already were subject to the Breach Notification Rule. Therefore, the notification requirements in the Breach Notification Rule are not duplicative.

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

The Privacy and Security Rules provide great flexibility to regulated entities, 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 Breach Notification Rule, the burden upon regulated entities of any size to provide the appropriate notifications occurs only when there has been a breach of unsecured PHI. Regulated entities have no obligations under the Breach Notification Rule in the absence of a breach. Further, regulated entities can prevent many breaches, and thus avoid the resulting Breach Notification Rule obligations, by implementing reasonable and appropriate protections for PHI in accordance with the Privacy and Security Rules.

**6. Consequences of Less Frequent Collection**

The changes to the Privacy Rule will result in a need for covered entities to perform the one-time information collection activities of revising and establishing policies and procedures, revising business associate agreements, updating their NPPs, and updating required training programs, for which documentation is required. A number of states are also likely to request an exception to federal preemption of contrary state law, resulting in an increased nonrecurring burden for that activity. In addition, covered entities will need to perform a recurring information collection activity when responding to requests for disclosures of PHI for which an attestation is required.

The frequency of the ongoing information collection requirements is a function of health care activities by regulated entities involving PHI, and the policies and procedures that they establish for complying with the HIPAA 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 for a period of 60 days under Regulation Identifier Number (RIN) 0945-AA20, 88 FR 23506 (April 17, 2023). A response to the submitted public comments is included with the final rule associated with this Information Collection Request (ICR).

**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 U.S.C. 552a) and the Freedom of Information Act (5 U.S.C. 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 regulated entities 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 estimated annual labor burden presented by the regulatory modifications in the first year of implementation, including nonrecurring and recurring burdens, is 4,584,224 burden hours at a cost of $582,242,165[7] and $20,910,207 of estimated annual labor costs in years two through five. The overall total burden for respondents to comply with the information collection requirements of the HIPAA Rules, including nonrecurring and recurring burdens presented by the program changes, is 953,982,236[8] burden hours at a cost of $107,336,706,167, plus $163,499,411 in capital costs for a total estimated annual burden of $107,500,205,579 in the first year following the effective date of the final rule. The total number of responses for the burden hours associated with this ICR is 1,154,350,069.[9] Details describing the burden analysis for the provisions of this rule are presented below.

**12A. Estimated Annualized Burden Hours**

Because of the number of changes to the Privacy Rule that affect the information collection, OCR presents in separate tables the existing collections (for which some estimates have been updated), new recurring collection burdens, and new nonrecurring collection 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,[10] the current calculation of costs reflects a lower number of individuals affected in 2022 breaches. 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

[7] This includes an increase of 416 burden hours and $38,705 in costs added to the existing information collection for requesting preemption exception determinations under 45 CFR 160.204.
[8] The total in ROCIS is 953,982,239. We attribute the difference to the effects of rounding.
[9]
[10] *See* https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201909-0945-001.

other cases provides 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 the Department believes this makes the calculations more transparent, it is not always obvious for any given provision which individuals or entities constitute the "respondents." Accordingly, OCR states the types of respondents in the table where appropriate. The estimated burden of a provision accrues to regulated entities for all but one burden category, where the Department indicates that the (voluntary) burden applies to individuals.

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

**Updated Burden Hours for Compliance with Existing Information Collections**

Table 1. This table shows updated data for existing information collections, reflecting hourly labor burdens that recur annually.

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours | Change from Approved ICR |
|---|---|---|---|---|---|---|---|
| 160.204 | Process for Requesting Exception Determinations (states or persons) - recurring | 1 | 1 | 1 | 16 | 16 | 0[q] |
| 164.308 | Risk Analysis - Documentation [2] | 1,774,331 | 1 | 1,774,331 | 10 | 17,743,310 | 743,310 |
| 164.308 | Information System Activity Review – Documentation | 1,774,331 | 12 | 21,291,972 | 0.75 | 15,968,979 | 668,979 |
| 164.308 | Security Reminders – Periodic Updates | 1,774,331 | 12 | 21,291,972 | 1 | 21,291,972 | 891,972 |
| 164.308 | Security Incidents (other than breaches) – Documentation | 1,774,331 | 52 | 92,265,212 | 5 | 461,326,060 | 19,326,060 |
| 164.308 | Contingency Plan—Testing and Revision | 1,774,331 | 1 | 1,774,331 | 8 | 14,194,648 | 594,648 |
| 164.308 | Contingency Plan—Criticality Analysis | 1,774,331 | 1 | 1,774,331 | 4 | 7,097,324 | 297,324 |
| 164.310 | Maintenance Records | 1,774,331 | 12 | 21,291,972 | 6 | 127,751,832 | 5,351,832 |
| 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 | 0 |
| 164.316 | Risk Analysis— | 1,774,331[b] | 1 | 1,774,331 | 10 | 17,743,310 | 743,310 |

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours | Change from Approved ICR |
|---|---|---|---|---|---|---|---|
| | Documentation, 164.308 | | | | | | |
| 164.316 | Information System Activity Review—Documentation, 164.308 | 1,774,331 | 12 | 21,291,972 | .75 | 15,968,979 | 668,979 |
| 164.316 | Security Reminders—Periodic Updates, 164.308 | 1,774,331 | 12 | 21,291,972 | 1 | 21,291,972 | 891,972 |
| 164.316 | Security Incidents—Other than breaches—Documentation, 164.308 | 1,774,331 | 52 | 92,265,212 | 5 | 461,326,060 | 19,326,060 |
| 164.316 | Documentation—Review and Update, 164.306 | 1,774,331 | 1 | 1,774,331 | 6 | 10,645,986 | 445,986 |
| 164.404 | Individual Notice—Written and E-mail Notice— Drafting | 64,592[c] | 1 | 64,592 | .5 | 32,296 | 3,055 |
| 164.404 | Individual Notice—Written and E-mail Notice— Preparing and documenting notification | 64,592 | 1 | 64,592 | .5 | 32,296 | 3,055 |
| 164.404 | Individual Notice—Written and E-mail Notice—Processing and sending | 64,592 | 650[d] | 42,004,718 | .008 | 336,038 | -572,070 |
| 164.404 | Individual Notice—Substitute Notice—Posting or publishing | 2,950[e] | 1 | 2,950 | 1 | 2,950 | 204 |
| 164.404 | Individual Notice—Substitute Notice—Staffing toll-free number | 2,950 | 1 | 2,950 | 1.18[f] | 3,481 | -5,910 |

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours | Change from Approved ICR |
|---|---|---|---|---|---|---|---|
| 164.404 | Individual Notice—Substitute Notice—Individuals' voluntary burden to call toll-free number for information | 41,760[g] | 1 | 41,760 | .125[h] | 5,220 | -8,938 |
| 164.406 | Media Notice | 626[i] | 1 | 626 | 1.25 | 783 | 449 |
| 164.408 | Notice to Secretary—Notice for breaches affecting 500 or more individuals | 626 | 1 | 626 | 1.25 | 783 | 449 |
| 164.408 | Notice to Secretary—Notice for breaches affecting fewer than 500 individuals | 63,966[j] | 1 | 63,966 | 1 | 63,966 | 5,751 |
| 164.410 | Business Associate notice to Covered Entity—500 or more individuals affected | 20 | 1 | 20 | 50 | 1,000 | 0 |
| 164.410 | Business Associate notice to Covered Entity— Less than 500 individuals affected | 1,165 | 1 | 1,165 | 8 | 9,320 | 0 |
| 164.414 | 500 or More Affected Individuals—Investigating and documenting breach | 626 | 1 | 626 | 50 | 31,300 | 17,950 |
| 164.414 | Less than 500 Affected Individuals—Investigating and documenting breach | 2,324 (breaches affecting 10-499 individuals) | 1 | 2,324 | 8 | 18,592 | -1,240 |
| 164.414 | Less than 500 Affected Individuals—Investigating and | 61,642 (breaches affecting <10 | 1 | 61,642 | 4 | 246,568 | 23,624 |

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours | Change from Approved ICR |
|---|---|---|---|---|---|---|---|
| | documenting breach | individuals) | | | | | |
| 164.508 | Uses and Disclosures – Organizational Requirements | 774,331 | 1 | 774,331 | 0.08333333 | 64,528 | 6,195 |
| 164.508 | Uses and Disclosures for Which Individual Authorization is Required | 774,331 | 1 | 774,331 | 1 | 774,331 | 74,331 |
| 164.512 | Uses and Disclosures for Research Purposes | 147,221[k] | 1 | 147,221 | 0.08333333 | 12,268 | 2,808 |
| 164.520 | Notice of Privacy Practices for Protected Health Information—Health plans —Periodic distribution of NPPs by paper mail | 150,000,000[l] | 1 | 150,000,000 | 0.00416666 [1 hour per 240 notices] | 625,000 | 208,333 |
| 164.520 | Notice of Privacy Practices for Protected Health Information—Health plans—Periodic distribution of NPPs by electronic mail | 150,000,000 | 1 | 150,000,000 | 0.00278333 [1 hour per 360 notices] | 417,500 | 139,167 |
| 164.520 | Notice of Privacy Practices for Protected Health Information—Health care providers—Dissemination | 613,000,000[m] | 1 | 613,000,000 | 0.05[n] | 30,650,000 | 0 |
| 164.522 | Rights to Request Privacy Protection for Protected Health Information | 40,000[n] | 1 | 40,000 | 0.05 | 2,000 | 1,000 |
| 164.524 | Access of Individuals to Protected Health Information— Copies | 615,000 | 1 | 615,000 | 0.05 | 30,750 | 20,750 |

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours | Change from Approved ICR |
|---|---|---|---|---|---|---|---|
| | of PHI[r] | | | | | | |
| 164.526 | Amendment of Protected Health Information— Requests | 150,000 | 1 | 150,000 | 0.08333333 | 12,500 | 0 |
| 164.526 | Amendment of Protected Health Information— Denials | 50,000 | 1 | 50,000 | 0.08333333 | 4,167 | 0 |
| 164.528 | Accounting for Disclosures of Protected Health Information | 5,000[o] | 1 | 5,000 | 0.05 | 250 | 0 |
| **TOTAL** | | | | **1,133,106,893** | | **949,398,012** | |

a. 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.
b. 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.
c. Total number of breach reports submitted to OCR in 2022.
d. Average number of individuals affected per breach incident reported in 2022.
e. This number includes all 626 large breaches and all 2,324 breaches affecting 10-499 individuals that were reported to OCR in 2022. Although some breaches involving fewer than 10 individuals may require substitute notice, the Department believes the costs of providing such notice through alternative written means or by telephone is negligible.
f. This assumes that 10% of the sum of (a) all individuals affected by large breaches (41,747,613) and (b) 5% of individuals affected by small breaches (.05 x 257,105 = 12,855) will require substitute notification. Thus, we calculate .10 * (41,747,613 + (.05 x 257,105)) = 4,176,047 affected individuals requiring substitute notification for an average of 1,416 affected individuals per such breach. [1,416 = 4,176,047/2,950]. We assume that 1% of the affected individuals per breach requiring substitute notice annually will follow up with a telephone call, resulting in 14.16 individuals per breach calling the toll-free number. We assume the call center staff will spend 5 minutes per call, with an average of 14 affected individuals per breach requiring substitute notice, resulting in 1.18 hours per breach spent answering calls from affected individuals.
g. As noted in the previous footnote, this number equals 1% of the affected individuals who require substitute notification (0.01 x 4,176,047 = 41,760).
h. 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.
i. The total number of breaches affecting 500 or more individuals for which OCR received reports in 2022.
j. The total number of breaches affecting fewer than 500 individuals for which OCR received reports in 2022.

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours | Change from Approved ICR |
|---|---|---|---|---|---|---|---|

k. The number of entities who use and disclose PHI for research purposes. The Department assumes a ratio of one U.S.-based research entity per study. *See* https://classic.clinicaltrials.gov/ct2/resources/trends#TypesOfRegisteredStudies (accessed March 13, 2024).
l. The Department assumes that half of the approximately 300,000,000 individuals insured by covered health plans will receive the plan's NPP by paper mail, and half will receive the NPP by electronic mail.
m. 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.
n. This represents 1 minute and fifteen seconds (75/3,600) to disseminate the NPP and 1 minute and 45 seconds for obtaining the signed patient acknowledgement.
o. The Department increased the estimated number of requests for confidential communications or restrictions on disclosures per year by 100 percent due to the combined effect of changes to the minimum necessary standard and the information blocking provisions of the ONC Cures Act Final Rule.
p. The Department estimates that covered entities annually fulfill 5,000 requests from individuals for an accounting of disclosures of their PHI.
q. The baseline burden of 16 hours for requesting exceptions from preemption remains unchanged; however, we have added a nonrecurring burden for this activity due to changes related to the legal status of reproductive health care. This is reported in a separate information collection and included in the table for new nonrecurring burdens below.
r. The Department estimates a total of 2.46 million requests for copies of PHI and assumes that half of those are individual access requests (1,240,000) and that half of the access requests are fulfilled through automated systems requiring no additional labor burden and half are fulfilled by workforce labor, resulting in an estimate of 615,000 access requests for an average of 3 minutes to fulfill each request.

**Burdens Hours for Compliance with New Information Collections, Recurring**

Table 2. This table shows new information collections as a result of the final rule, reflecting hourly labor burdens that recur annually.

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response | Total Burden Hours |
|---|---|---|---|---|---|---|
| 164.509 | Disclosures for which attestation is required | 2,794,201 | 1 | 2,794,201 | 0.083 | 232,850 |
| 164.509 | Attestations requiring investigation review | 1,300 | 1 | 1,300 | 1 | 1,300 |
| 164.509 | Attestations | 325 | 1 | 325 | 3 | 975 |

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response | Total Burden Hours |
|---|---|---|---|---|---|---|
| | requiring additional action | | | | | |
| **TOTAL** | | | | **2,795,826** | | **235,125** |

**Burden Hours for Compliance with New Information Collections, Nonrecurring**

Table 3. This table shows estimated burden hours for new information collections, incurred on a one-time basis within the first year of compliance with the final rule.

| 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) | 26 | 1 | 26 | 16 | 416 |
| 164.504 | Revising Business Associate Agreements | 350,000[a] | 1 | 350,000 | 1 | 350,000 |
| 164.520 | Notice of Privacy Practices for Protected Health Information—Update the notice | 774,331 | 1 | 774,331 | 0.83 | 645,276 |
| 164.520 | Notice of Privacy Practices for Protected Health Information—Mailing notice to 10% of subscribers at a rate of 240 notices/hour | 15,000,000 | 1 | 15,000,000 | 0.0042 | 62,500 |
| 164.520 | Notice of Privacy Practices for Protected Health Information— | 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 |
|---|---|---|---|---|---|---|
| | Post updated notice online | | | | | |
| 164.530 | Administrative Requirements—Policies & Procedures (new and updated) | 774,331 | 1 | 774,331 | 2.5 | 1,935,828 |
| 164.530 | Administrative Requirements—Training — 164.525 Update training content | 774,331 | 1 | 774,331 | 1.5 | 1,161,497 |
| **TOTAL** | | | | 18,447,350 | | **4,349,099** |

a. Respondents for this item are the number of revised business associate agreements.

## Total Burden Hours of All Information Collections

Table 4.

| Burden Tables | Total Number of Responses | Total Burden Hours |
|---|---|---|
| Table 1. Burden Hours of Existing Information Collections | 1,133,106,893 | 949,398,012 |
| Table 2. Burden Hours of New Information Collections, Recurring | 2,795,826 | 235,125 |
| Table 3. Burden Hours of New Information Collections, Nonrecurring | 18,447,350 | 4,349,099 |
| **Total for the HIPAA Rules** | **1,154,350,069** | **953,982,236** |

**12B. Estimated Annualized Burden Costs**

The total cost of this information collection, apart from capital costs, is approximately $107,336,706,168. These figures are based on hourly wages. Benefits are calculated by multiplying the base hourly wage rate by two.

**Updated Costs of Compliance with Existing Information Collections**

Table 5. The table below shows the updated costs that are incurred annually to comply with the existing information collections. All existing information collections are recurring.

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.308 | Risk Analysis – Documentation | 17,743,310 | $115.26[11] | $2,045,093,911 |
| 164.308 | Information System Activity Review – Documentation | 15,968,979 | $115.26 | $1,840,584,520 |
| 164.308 | Security Reminders – Periodic Updates | 21,291,972 | $115.26 | $2,454,112,693 |
| 164.308 | Security Incidents – Other than breaches – Documentation | 461,326,060 | $115.26 | $53,172,441,676 |
| 164.308 | Contingency Plan – Testing and Revision | 14,194,648 | $115.26 | $1,636,075,128 |

[11] The $115.26 wage, which includes $57.63 plus 100% for benefits, applies to the category “Information Security Analysts.”

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.308 | Contingency Plan – Criticality Analysis | 7,097,324 | $115.26 | $818,037,564 |
| 164.310 | Maintenance Records | 127,751,832 | $100.64[12] | $12,856,944,372 |
| 164.314 | Security Incidents – Business Associate reporting of non-breach incidents to Covered Entities | 240,000,000 | $115.26 | $27,662,400,000 |
| 164.316 | Documentation – Review and Update | 10,645,986 | $115.26 | $1,227,056,346 |
| 164.404 | Individual Notice—Written and E-mail Notice— Drafting | 32,296 | $93.04 | $3,004,820 |
| 164.404 | Individual Notice—Written and E-mail Notice— Preparing and documenting notification | 32,296 | $43.80[13] | $1,414,565 |
| 164.404 | Individual Notice—Written and E-mail Notice— Processing and sending | 336,038 | $43.80 | $14,718,453 |
| 164.404 | Individual Notice—Substitute Notice — Posting or publishing | 2,950 | $97.82[14] | $288,569 |
| 164.404 | Individual Notice—Substitute Notice — Staffing toll-free number | 3,481 | $43.80 | $152,468 |
| 164.404 | Individual Notice—Substitute Notice — Individuals burden to call toll-free number for information | 5,220 | $59.52[15] | $310,698 |
| 164.406 | Media Notice | 783 | $80.08[16] | $62,666 |

[12] The $100.64 wage, which includes $50.32 plus 100% for benefits, applies to "Management Analysts."
[13] The $43.80 wage, including $21.90 plus 100% for benefits, applies to "Office and Administrative Support Occupations."
[14] The $97.82 wage, including $48.91 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.
[15] The $59.52 wage, including $29.76 plus 100% for benefits, is the mean wage for "All Occupations."

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.408 | Notice to Secretary— Notice for breaches affecting 500 or more individuals | 783 | $80.08 | $62,6 |
| 164.408 | Notice to Secretary— Notice for breaches affecting fewer than 500 individuals | 63,966 | $43.80 | $2,801,711 |
| 164.410 | Business Associate notice to Covered Entity - 500 or more individuals affected | 1,000 | $123.06[17] | $123,060 |
| 164.410 | Business Associate notice to Covered Entity – Less than 500 individuals affected | 9,320 | $123.06 | $1,146,919 |
| 164.414 | 500 or More Affected Individuals – Investigating and documenting breach | 31,300 | $123.06 | $3,851,778 |
| 164.414 | Less than 500 Affected Individuals – Investigating and documenting breach | 18,592 (for breaches affecting 10-499 | $123.06 | $2,287,932 |
| | | 246,568 (for breaches affecting <10 individuals) | $123.06 | $30,342,658 |
| 164.504 | Uses and Disclosures – Organizational Requirements | 64,528 | $93.04 | $6,003,646 |
| 164.508 | Uses and Disclosures for Which Individual authorization is required | 774,331 | $93.04 | $72,043,756 |
| 164.512 | Uses and Disclosures for Research Purposes | 12,268 | $93.04 | $1,141,453 |
| 164.520 | Notice of Privacy Practices for | 625,000 | $43.80 | |

[16] The $80.08 average cost per hour is derived by calculating the cost for 626 hours for a GS-12 equivalent ($64.04 wage, including $32.02 plus 100% for benefits) and 156.5 hours for a Public Relations Manager ($144.26 per hour including benefits) and dividing the sum by the total number of burden hours.
[17] The $123.06 wage, including $61.53 plus 100% for benefits, applies to "Medical and Health Services Manager."

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| | Protected Health Information – Health plans – periodic distribution of NPPs by paper mail | | | $27,375,000 |
| 164.520 | Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by electronic mail | 417,500 | $43.80 | $18,286,500 |
| 164.520 | Notice of Privacy Practices for Protected Health Information (health care providers – dissemination and acknowledgement) | 30,650,000 | $93.04 | $2,851,676,000 |
| 164.522 | Rights to Request Privacy Protection for Protected Health Information | 2,000 | $93.04 | $186,080 |
| 164.524 | Access of Individuals to Protected Health Information (disclosing copies of PHI to individuals) | 30,750 | $93.04 | $2,860,980 |
| 164.526 | Amendment of Protected Health Information (requests) | 12,500 | $93.04 | $1,163,000 |
| 164.526 | Amendment of Protected Health Information (denials) | 4,167 | $93.04 | $387,667 |
| 164.528 | Accounting for Disclosures of Protected Health Information | 250 | $93.04 | $23,260 |
| **TOTAL** | | | | **$106,754,464,003** [18] |

[18] Total may not add up due to rounding.

**Costs of Compliance with New Information Collections, Recurring**

Table 6. The table below shows the annual costs of complying with new burdens that will recur.

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.509 | Uses and disclosures for which attestation is required--recurring burden | 232,850 | $88.41 | $20,585,500 |
| 164.509 | Attestations requiring investigation review | 1,300 | $157.48 | $204,724 |
| 164.509 | Attestations requiring additional action | 975 | $123.06 | $119,984 |
| **TOTAL** | | | | **$20,910,207** |

**Costs of Compliance with New Information Collections, Nonrecurring**

Table. 7. The table below shows the costs that will be incurred within the first year of compliance with the final rule and that will not recur.

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 160.204 | Process for Requesting Exception Determinations | 416 | $93.04 | $38,705 |
| 164.504 | Revising business associate agreements | 350,000 | $157.48 | $55,118,000 |
| 164.520 | Revising the Notice of Privacy Practices | 645,276 | $157.48 | $101,618,038 |
| 164.520 | Mailing notice to 10% of subscribers at a rate of 240 notices/hour | 62,500 | $43.80 | $2,737,500 |
| 164.520 | Post New NPP Online | 193,583 | $97.82 | $18,936,265 |
| 164.530 | Update policies & procedures | 1,935,828 | $157.48 | $304,854,115 |
| 164.530 | Update HIPAA Training Program | 1,161,497 | $67.18 | $78,029,335 |
| **TOTAL** | | | | **$561,331,957** |

**Total Costs of Compliance with All Information Collections**

Table 8. The table below shows the total of all labor costs for the information collection request.

| Cost Tables | Cost Totals |
|---|---|
| Table 5, Costs of Existing Burdens | $106,754,464,003 |
| Table 6, Costs of New Burdens, Recurring | $20,910,207 |
| Table 7, Costs of New Burdens, Nonrecurring | $561,331,957 |
| **TOTAL OF ALL HOURLY LABOR COSTS** | **$107,336,706,168**[19] |

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

The total capital cost is $163,499,411. The capital cost for providing the required breach notifications is $18,656,911. Capital costs of $144,842,500 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**

Table 9.

| Section | Cost Elements | Number of Breaches | Cost per Breach | Total Cost |
|---|---|---|---|---|

[19] Totals may not add due to the effects of rounding.

| | | | | |
|---|---|---|---|---|
| 164.404 | Individual Notice—Postage, Paper, and Envelopes | 64,592 | $263.95[20] | $17,049,295 |
| 164.404 | Individual Notice—Substitute Notice Media Posting | 2,950[21] | $480 | $1,416,000 |
| 164.404 | Individual Notice—Substitute Notice—Toll-Free Number | 2,950 | $64.95[22] | $191,616 |
| **Section** | **Cost Elements** | **Number of NPPs** | **Average Cost per NPP** | **Total NPP Costs** |
| 164.520 | Printing for Notice of Privacy Practices for Protected Health Information (health plans) | 150,000,000 | $.18 | $26,340,000[23] |
| 164.520 | Postage and Envelope for Notice of Privacy Practices for Protected Health Information (health plans) | 15,000,000 | $.72 | $10,859,700[24] |
| 164.520 | Printing Notice of Privacy Practices for Protected Health Information (health care providers) | 613,000,000 | $.18 | $107,642,800[25] |
| **Total** | | | | **$163,499,411[26]** |

[20] OCR again assumes that half of all affected individuals (half of 42,004,718 equals 21,002,359) will receive paper notification and half will receive notification by email. Therefore, on average, 325 individuals per breach will receive notification by mail. Further, OCR estimates that each mailed notice will cost $.05 for paper and envelope, $.08 for printing, and $.68 for postage. Accordingly, on average, the capital cost for mailed notices for each breach is $.81 for each of 325 notices, or $263.95.

[21] The number of breaches requiring substitute notice equals all 626 large breaches and all 2,324 breaches affecting 10-499 individuals.

[22] 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.

[23] This number is based on the assumption that each of 150 million paper notices costs $.1756 to print ($.0256 per sheet of paper plus $.15 for printing), for a total of $26.3 million in printing costs.

[24] This number results from the following assumptions: 10% of 150 million notices (15,000,000) will be mailed separately from regular health plan mailings; and each separately mailed paper notice costs $.72 ($.04 for envelope plus $.68 for postage), for a total of $10.8 million in mailing costs.

[25] This estimate includes 613 million notices with a combined cost for paper and printing of $.18 per notice.

[26] Total may not add up due to rounding.

**14. Annualized Cost to Federal Government**

The Privacy and Security Rules require regulated entities to collect, maintain, and disclose information to comply with the Rules' requirements. However, OCR generally does not collect and store this information, nor does OCR require regulated entities 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 pursuant to the Breach Notification Rule falls upon regulated entities. OCR does not produce or provide regulated entities 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 regulated entities. The costs to regulated entities that are Federal entities are included among the overall burden estimates for regulated entities, and thus are not addressed here. There is otherwise no cost to the Federal Government for this portion of the information collection.

However, OCR is required 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 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. The annual recurring cost to the federal government for the breach portal is approximately $216,000.

The Department further expects that it may incur a 26-fold increase in the number of requests for exceptions from preemption of state law in the first year after the rule becomes effective, at an estimated total cost of approximately $146,319 for an average cost of $7,410 per request. This increase is based on the number of states that have or are likely to pass more restrictive reproductive health care laws[27] and may seek to use or disclose individuals' PHI to enforce those laws. This estimate assumes that the Department receives and reviews exception requests from each of those 26 states, that half of those require a more complex analysis, and that all requests result in a written response within one year of the final rule's publication. This is a non-recurring cost to the government.

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

The rule associated with this ICR establishes program changes since the previous information collection submission, and thus this information collection reflects new requirements for regulated entities and does not create any modified burdens and quantifiable savings for individuals. The Department adjusts the Privacy Rule to strengthen privacy protections for individuals' PHI by:

**1)** Adding a new category of prohibited uses and disclosures.

**2)** Revising or clarifying certain definitions and terms that apply to the Privacy Rule, as well as other HIPAA Rules.

[27] *See* Lawrence O. Gostin et al., "One Year After *Dobbs*—Vast Changes to the Abortion Legal Landscape," 4(8) JAMA Health Forum (2023), https://jamanetwork.com/journals/jama-health-forum/fullarticle/2808205 (counting 21 states with post-*Dobbs* limits that are more restrictive than *Roe* v. *Wade* allowed) and Laura Deal, "State Laws Restricting or Prohibiting Abortion," Congressional Research Service (January 22, 2024), https://crsreports.congress.gov/product/pdf/R/R47595. Because of the pace of change in this area, the Department relies on a higher number than JAMA's 2023 figure as a basis for its cost estimates.

3) Clarifying that a regulated entity may not decline to recognize a person as a personal representative for the purposes of the Privacy Rule solely because they provide or facilitate reproductive health care for an individual.

4) Adding a new requirement that, in certain circumstances, a regulated entity must first obtain an attestation from a person requesting PHI that the requested use or disclosure is not for certain purposes.

5) Modifying the content requirements of the NPP to inform individuals that their PHI may not be used or disclosed for certain purposes, and that their 42 CFR part 2 information will be protected.

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

1) Increasing the number of respondents requesting exceptions to state law preemption under 45 CFR 160.204 from 1 to 27 based on an expected reaction by states that have enacted restrictions on reproductive health care access.

2) Increasing the number of covered entities from 700,000 to 774,331 due to program change.

3) Increasing the burden hours by a factor of two for responding to individuals' requests for restrictions on disclosures of their PHI under 45 CFR 164.522 to represent a doubling of the expected requests.

4) Updating the number of breaches for which notification is required to reflect data in OCR's 2022 Report to Congress[28] and related burdens.

[28] *See* Off. for Civil Rights, "Annual Report to Congress on Breaches of Unsecured Protected Health Information," U.S. Dep't of Health and Human Servs. (2022), https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html.

5) Increasing the number of estimated uses and disclosures for research purposes.

6) Increasing the annual burden for distributing health plan NPPs to a percentage of health plan subscribers due to a 50% increase in the number of Americans with health coverage, for a total of 300,000,000 health plan NPPs. This results in the following changes:

    i. increasing to 150,000,000 the number of NPPs mailed by health plans

    ii. increasing to 150,000,000 the number of NPPs electronically distributed by health plans

    iii. increasing to 15,000,000 the number of NPPs mailed by health plans that do not do an annual mailing and need to conduct an off-cycle mailing as a result of program changes.

In addition to these changes, the Department added new burdens as a result of the program changes in the final rule:

1) A nonrecurring burden of 1 hour for each of 350,000 business associate agreements that is likely to be revised to address respective responsibilities of covered entities and their release-of-information contractors for handling requests for PHI under 45 CFR 164.512(d), (e), (f), and (g)(1).

2) A recurring burden of 5 minutes per request for staff to determine whether an attestation is required for disclosure under 45 CFR 164.509.

3) A recurring burden of 1 hour per request for legal review of whether certain requests identified by staff as potentially pertaining to the lawfulness of reproductive health care.

**4)** A recurring burden of 3 hours per request for a percentage of requests requiring legal review that might require additional manager review to determine whether the requirements at 45 CFR 164.509 are met.

**5)** A nonrecurring burden of 50 minutes per covered entity to update the required content of its NPP under 45 CFR 164.520.

**6)** A nonrecurring burden of 15 minutes per covered entity for posting an updated NPP online under 45 CFR 164.520.

**7)** A nonrecurring burden for mailing NPP to a percentage of health plan subscribers at a rate of 240 notices per hour under 45 CFR 164.520.

**8)** A nonrecurring burden of 2.5 hours for each covered entity to update its policies and procedures under 45 CFR 164.530.

**9)** A nonrecurring burden of 90 minutes for each covered entity to update the content of its HIPAA training program under 45 CFR 164.530.

As a result, the total estimated annual labor and capital costs associated with compliance with the HIPAA Rules' information collections (including nonrecurring costs), apart from costs to the Federal Government, have increased from $66,812,896,048 to $107,492,846,352.

**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 Privacy, Security, and Breach Notification Rules as described above in part A do not require the application of statistical methods.