**Supporting Statement for**

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

## 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 or "Department") is requesting OMB approval for the revision of a previously approved OCR information collection, OMB #0945-0003.[1] The Department is initiating rulemaking to modify existing standards for security of electronic protected health information (ePHI) established under the Health Insurance Portability and Accountability Act (HIPAA) of 1996[2] and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).[3] This information collection also addresses standards for privacy and breach notification established under HIPAA, the HITECH Act, and the Genetic Information Nondiscrimination Act of 2008 (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' PHI and rights of individuals with respect to their PHI. The information collections in the HIPAA Rules include requirements for recordkeeping, reporting, and third-party disclosures.

[1] ICR ref. no. 202401-0945-002.
[2] Pub. L. 104–191, 110 Stat. 1936 (Aug. 21, 1996) (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, 123 Stat. 115 (Feb. 17, 2009) (codified at 42 U.S.C. 201 note).
[4] Title I, section 105, Pub. L. 110–233, 122 Stat. 881 (May 21, 2008) (codified at 42 U.S.C. 2000ff).

The proposed rule would modify the security standards to better protect the confidentiality, integrity, and availability of ePHI. The proposals in the Notice of Proposed Rulemaking (NPRM) would strengthen the cybersecurity of ePHI by: (1) clarifying and providing more specific instruction about what covered entities and their business associates (collectively, "regulated entities") must do to ensure the security of ePHI; (2) requiring that policies and procedures be in writing, reviewed, tested, and updated on a regular basis; and (3) improving the Security Rule's alignment with best practices in cybersecurity.

As a result of updated statistics for the number of covered entities and the proposed regulatory modifications, OCR requests approval to update and add certain burden estimates to the information collections associated with the HIPAA Rules.

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

The HIPAA Security Rule ("Security Rule") requires that regulated entities maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI; protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI; 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 with the Security Rule.

The HIPAA Privacy Rule ("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 covered providers who have a direct treatment relationship with individuals and health plans. Accordingly, covered entities are required to provide certain information to individuals. They are also required 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 with the Privacy Rule.

The HIPAA Breach Notification Rule ("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 prominent media outlets 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 with the Breach Notification Rule.

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 with different levels of technological sophistication to comply with the requirements of the regulations. Thus, under the Security Rule, regulated entities are empowered to determine the specific risks and vulnerabilities to ePHI in their circumstances and to implement safeguards in a manner that is reasonable and appropriate for their particular environments. Regulated entities that are subject to the Security Rule's requirements are permitted to maintain the required documentation in electronic or paper form. The Security Rule permits regulated entities to consider several factors, including their technical infrastructure, hardware, and software security abilities. As cybersecurity technology has improved, costs to implement certain technology have decreased. For example, regulated entities are required to address whether to encrypt ePHI or implement another mechanism to achieve similar protections. Today, encryption is built into most software, and where it is not, there are affordable and easily implemented solutions for encrypting sensitive information.

The Privacy Rule allows covered entities 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 Breach Notification Rule permits individual notification of a breach by electronic means. Specifically, 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. The Security Rule's standards for safeguarding ePHI are consistent with certain other security frameworks and requirements, such as those published by the National Institute of Standards and Technology (which apply to Federal Government entities, including some covered entities). In certain cases, activities performed in compliance with other security frameworks might fulfill an equivalent Security Rule requirement, and thus the particular Security Rule requirement would not create an additional burden in this respect. In contrast, many requirements of the Security Rule, including its documentation requirements, 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 in the security of personal information. However, many of these laws do not specifically require notification following the breach of PHI as defined by HIPAA. Even in cases where a breach of PHI would trigger notification under both state law and HIPAA, the Department believes that both the state law notification and the notification under this rule can be satisfied with a single breach notification.

**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, complexity, and capabilities of each regulated entity and the potential risks to PHI.

With regard to the Breach Notification Rule, regulated entities are only required to provide the appropriate notifications 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 can 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 proposed changes to the Security Rule would result in a need for regulated entities to perform the one-time information collection activities of: (1) deploying multi-factor

authentication; (2) segmenting networks; (3) revising and establishing policies and procedures; (4) revising business associate agreements; (5) revising group health plan documents; and (6) updating required training programs, for which documentation is required.

Additionally, the proposed changes to the Security Rule would result in ongoing information collections of: (1) conducting a Security Rule compliance audit; (2) providing verification of business associates' compliance with technical safeguards; (3) obtaining written verification from their business associates or subcontractors that the business associates or subcontractors, respectively, have conducted the required verification of compliance with technical safeguards; (4) providing notification of termination or change of workforce members' access to ePHI; (5) disabling unused ports and removing extraneous software; (6) deploying penetration testing; and (7) notifying regulated entities upon activation of a contingency plan.

For the first time, the Department is including proposed changes to the Security Rule that would result in health plan sponsors performing information collection activities of: (1) performing and documenting a risk analysis; (2) documenting a review of information system activity; (3) providing ongoing education for workforce members; (4) documenting security incidents (other than breaches); (5) testing and revising a contingency plan; (6) conducting a criticality analysis for a contingency plan; (7) notifying group health plans of workforce members' termination of access to ePHI; (8) creating regular maintenance records; (9) deploying multi-factor authentication; (9) disabling unused ports and removing extraneous software as part of configuration management; (10) deploying penetration testing; and (11) notifying group health plans upon activation of a contingency plan.

The frequency of the ongoing information collection requirements is a function of activities carried out by regulated entities that involve PHI and the policies and procedures that such regulated entities establish to comply with the HIPAA Rules. It is also a function of the Department's need to examine regulated entities' policies and procedures for compliance and enforcement purposes, such as to evaluate a complaint made by an individual against a regulated entity. 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 each breach affecting more than 500 residents of a state or jurisdiction, and notification to the Secretary of HHS within a certain amount of time after each breach (within 60 days after discovery for breaches affecting 500 or more individuals and annually for breaches affecting less than 500 individuals). 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-AA22, XX FR XXX (Date).

**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 about breaches of unsecured PHI affecting more than 500 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 proposed regulatory modifications is 77,067,552 burden hours at a first-year cost of $9,314,106,174. These figures, respectively, represent the sum of 37,781,637 new burden hours at a cost of $4,655,324,954 for compliance by regulated entities and 39,285,915 new burden hours at a cost of $4,658,781,219 for compliance by health plan sponsors.

The overall total burden for respondents to comply with the information collection requirements of the HIPAA Rules, including new burdens presented by the proposed program changes, is estimated to be 925,144,023[5] burden hours at a cost of $109,085,104,674, plus $163,499,411 in

[5] The figure in ROCIS is 925,144,026, and the difference is due to rounding.

capital costs for a total estimated annual burden of $109,248,604,085 after the effective date of the final rule. This estimate is based on a total of 1,202,562,864 responses for a total of 2,565,011 respondents. The total burden for the HIPAA Rules, including the proposed changes proposed in this NPRM, would result in a decrease of 28,838,213 burden hours and a cost increase of $1,911,898,144 in comparison to the baseline in the ICR associated with the 2024 Privacy Rule to Support Reproductive Health Care Privacy. This decrease in burden hours is the result of several adjustments, including reducing the estimated number of hours for the reporting of security incidents other than breaches and removing the hours for one-time costs attributable to the 2024 Privacy Rule. Despite the decrease in burden hours, estimated costs have increased because of inflation in wage rates. Details describing the burden analysis for the provisions of this rule are presented below.

**12A. Estimated Annualized Burden Hours**

Because of the number of proposed changes to the Security Rule that affect the information collection, OCR presents in separate tables the existing collections (for which some estimates have been updated) and new 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 remain unchanged since the previously approved information collection.[6] 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 at other times, provides an estimate of individuals who are affected by entities' compliance activities or exercise an individual right under the Rules. Although the Department believes this

[6] *See* "View ICR," Office of Information and Regulatory Affairs, Office of Management and Budget (July 9, 2024), https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202401-0945-002.

makes the calculations more transparent, it is not always obvious for any given provision which entities (or, in one case, individuals) constitute the “respondents.” Accordingly, OCR states the types of respondents in the table where appropriate.

In this NPRM, the Department is including estimates of potential costs for health plan sponsors to comply with the administrative, physical, and technical safeguards of the Security Rule for the first time. Group health plans would be required to update plan documents to require compliance by health plan sponsors with the administrative, physical, and technical safeguards in the Security Rule and notification of group health plans when health plan sponsors activate their contingency plan.

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 Regulated Entities' Compliance with Existing Information Collections**

Table 1. This table shows updated data for existing information collections for regulated entities,[7] 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) | 1 | 1 | 1 | 16 | 16 | -416[b] |
| 164.308 | Risk Analysis—Documentation[c] | 1,822,600 | 1 | 1,822,600 | 10 | 18,226,000 | 482,690 |
| 164.308 | Information System Activity Review – Documentation | 1,822,600 | 12 | 21,871,200 | 0.75 | 16,403,400 | 434,421 |
| 164.308 | Ongoing Education | 1,822,600 | 12 | 21,871,200 | 1 | 21,871,200 | 579,228 |
| 164.308 | Security Incidents (Other than Breaches) —Documentation | 1,822,600 | 52 | 94,775,200 | 5 | 473,876,000 | 12,549,940 |
| 164.308 | Contingency Plan—Testing and Revision | 1,822,600 | 1 | 1,822,600 | 8 | 14,580,800 | 386,152 |
| 164.308 | Contingency Plan—Criticality Analysis | 1,822,600 | 1 | 1,822,600 | 4 | 7,290,400 | 193,076 |
| 164.310 | Maintenance Records | 1,822,600 | 12 | 21,871,200 | 6 | 131,227,200 | 3,475,368 |
| 164.314 | Security Incidents—Business Associate | 1,000,000 | 12 | 12,000,000 | 10 | 120,000,000 | -120,000,000 |

[7] In one instance, the table shows burdens for individuals to voluntarily call an information line.

| 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 |
|---|---|---|---|---|---|---|---|
| | Reporting of Non-breach Incidents to Covered Entities | | | | | | |
| 164.316 | Documentation—Review and Update | 1,822,600 | 1 | 1,822,600 | 6 | 10,935,600 | 289,614 |
| 164.404 | Individual Notice—Written and E-mail Notice— Drafting | 64,592[d] | 1 | 64,592 | 0.5 | 32,296 | 0 |
| 164.404 | Individual Notice—Written and E-mail Notice— Preparing and Documenting Notification | 64,592 | 1 | 64,592 | 0.5 | 32,296 | 0 |
| 164.404 | Individual Notice—Written and E-mail Notice—Processing and Sending | 64,592 | 650[e] | 42,004,718 | 0.008 | 336,038 | 0 |
| 164.404 | Individual Notice—Substitute Notice—Posting or Publishing | 2,950[f] | 1 | 2,950 | 1 | 2,950 | 0 |
| 164.404 | Individual Notice—Substitute Notice—Staffing toll-free number | 2,950 | 1 | 2,950 | 1.18[g] | 3,481 | 0 |
| 164.404 | Individual Notice—Substitute Notice—Individuals' Voluntary Burden to Call Toll-free Number for Information | 41,760[h] | 1 | 41,760 | 0.125[i] | 5,220 | 0 |
| 164.406 | Media Notice | 626[j] | 1 | 626 | 1.25 | 783 | 0 |
| 164.408 | Notice to Secretary—Notice for Breaches Affecting 500 or More Individuals | 626 | 1 | 626 | 1.25 | 783 | 0 |

| 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 |
|---|---|---|---|---|---|---|---|
| 164.408 | Notice to Secretary—Notice for Breaches Affecting Fewer than 500 Individuals | 63,966[k] | 1 | 63,966 | 1 | 63,966 | 0 |
| 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 | 0 |
| 164.414 | Less than 500 Affected Individuals—Investigating and Documenting Breach | 2,324 (breaches affecting 10-499 individuals) | 1 | 2,324 | 8 | 18,592 | 0 |
| 164.414 | Less than 500 Affected Individuals—Investigating and Documenting Breach | 61,642 (breaches affecting <10 individuals) | 1 | 61,642 | 4 | 246,568 | 0 |
| 164.508 | Uses and Disclosures—Organizational Requirements | 822,600 | 1 | 822,600 | 0.08333333 | 68,550 | 4,022 |
| 164.508 | Uses and Disclosures for Which Individual Authorization is Required | 822,600 | 1 | 822,600 | 1 | 822,600 | 48,269 |

| 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 |
|---|---|---|---|---|---|---|---|
| 164.509 | Disclosures for Which Attestation is Required —Recurring Burden | 2,794,201 | 1 | 2,794,201 | 0.08333333 | 232,850 | 0 |
| 164.509 | Attestation Investigation Review | 1,300 | 1 | 1,300 | 1 | 1,300 | 0 |
| 164.509 | Attestation Requiring Additional Action | 325 | 1 | 325 | 3 | 975 | 0 |
| 164.512 | Uses and Disclosures for Research Purposes | 153,857[l] | 1 | 153,857 | 0.08333333 | 12,821 | 553 |
| 164.520 | Notice of Privacy Practices for Protected Health Information— Health Plans— Periodic Distribution of NPPs by Paper Mail | 150,000,000 [m] | 1 | 150,000,000 | 0.00416666 [1 hour per 240 notices] | 625,000 | 0 |
| 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 | 0 |
| 164.520 | Notice of Privacy Practices for Protected Health Information— Health Care Providers— Dissemination and Acknowledgement | 613,000,000[n] | 1 | 613,000,000 | 0.05[o] | 30,650,000 | 0 |
| 164.522 | Rights to Request Privacy Protection for Protected Health Information | 40,000[p] | 1 | 40,000 | 0.05 | 2,000 | 0 |
| 164.524 | Access of Individuals to Protected Health Information— Copies | 615,000 | 1 | 615,000 | 0.05 | 30,750 | 0 |

| 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[q] | | | | | | |
| 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[r] | 1 | 5,000 | 0.05 | 250 | 0 |
| **TOTAL** | | | | **1,140,446,641** | | **848,076,471** | |

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 the requirements of the Security Rule, while large entities may spend more hours than those provided here because of their size and complexity.
b. The baseline burden of 16 hours for requesting exceptions from preemption remains unchanged; however, we have decreased the number of estimated requests for an exception to federal preemption of state law to the prior baseline of 1 request per year.
c. This estimate includes 822,609 estimated covered entities and 1 million estimated business associates. The burden analysis for the Omnibus HIPAA Final Rule estimated that there were 1-2 million business associates. 78 FR 5566, 5669-5670 (Jan. 25, 2013). 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.
d. Total number of breach reports submitted to OCR in 2022.
e. Average number of individuals affected per breach incident reported in 2022.
f. This number includes all 626 breaches affecting 500 or more individuals (referred to herein as “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.
g. 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) would 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 would follow up with a telephone call, resulting in 14.16 individuals per breach calling the toll-free number. We assume the call center staff would 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.
h. As noted in the previous footnote, this number equals 10% of the sum of all individuals affected by large breaches and 5% of individuals affected by small breaches by 1%. [(.10 * (41,747,613 + (.05 x 257,105))) * .01 = 41,760].
i. 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.

j. The total number of breaches affecting 500 or more individuals for which OCR received reports in 2022.
k. The total number of breaches affecting fewer than 500 individuals for which OCR received reports in 2022.
l. 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* "Trends and Charts on Registered Studies: Percentage of registered studies by location," National Library of Medicine, National Institutes of Health, U.S. Department of Health and Human Services, https://clinicaltrials.gov/about-site/trends-charts (accessed Nov. 13, 2024).
m. The Department assumes that half of the approximately 300,000,000 individuals insured by covered health plans would receive the plan's NPP by paper mail, and half would receive the NPP by electronic mail.
n. The Department estimates that each year covered health care providers would have first-time visits with 613 million individuals, to whom the providers must give an NPP.
o. 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.
p. The Department increased the estimated number of requests for confidential communications or restrictions on disclosures per year by 100 percent because of the combined effect of changes to the minimum necessary standard and the information blocking provisions of the ONC Cures Act Final Rule.
q. 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.
r. The Department estimates that covered entities annually fulfill 5,000 requests from individuals for an accounting of disclosures of their PHI.

**Burdens Hours for Regulated Entities' Compliance with New Information Collections**

Table 2. This table shows new information collections for regulated entities as a result of the proposed rule.

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours |
|---|---|---|---|---|---|---|
| 164.308 | Security Rule Compliance Audit | 1,822,600 | 1 | 1,822,600 | 2 | 3,645,200 |
| 164.308 | Business Associate Verification of Technical Safeguards | 1,000,000 | 1 | 1,000,000 | 2 | 2,000,000 |
| 164.308 | Covered Entity's Obtain Business Associate Compliance | 822,600 | 1 | 822,600 | 0.50 | 411,300 |

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours |
|---|---|---|---|---|---|---|
| | Verification[b] | | | | | |
| 164.308 | Business Associate Obtain Subcontractors' Compliance Verification | 1,000,000 | 1 | 1,000,000 | 0.08 | 83,333 |
| 164.308 | Notification of Workforce Members' Termination of Access to ePHI | 1,822,600 | 1 | 1,822,600 | 1 | 1,822,600 |
| 164.308 | Update Workforce Training | 1,822,600 | 1 | 1,822,600 | 2 | 3,645,200 |
| 164.308 | Update Business Associate Agreements[c] | 1,822,600 | 1 | 1,822,600 | 1 | 1,822,600 |
| 164.312 | Multi-factor Authentication | 1,822,600 | 1 | 1,822,600 | 1.5 | 2,733,900 |
| 164.312 | Network Segmentation | 1,822,600 | 1 | 1,822,600 | 4.5 | 8,201,700 |
| 164.312 | Configuration Management | 1,395,396 | 1 | 1,395,396 | 0.5 | 697,698 |
| 164.312 | Penetration Testing | 1,822,600 | 1 | 1,822,600 | 3 | 5,467,800 |
| 164.308<br>164.310<br>164.312 | Revise Policies and Procedures | 1,822,600 | 1 | 1,822,600 | 3.5 | 6,379,100 |
| 164.314 | Notification of Contingency Plan Activation | 1,000,000 | 1 | 1,000,000 | 0.5 | 500,000 |
| 164.314 | Revise Health Plan Documents | 6,162 | 120 | 742,411 | 0.5 | 371,206 |
| **TOTAL** | | | | **20,541,207** | | **37,781,637** |

a. The figures in this column are averages based on a range. Small entities may require fewer hours to conduct certain compliance activities, particularly those required by the Security Rule, while large entities may spend more hours than those provided here because of their size and complexity.
b. The number of respondents is the number of business associate agreements to be revised.
c. We did not include the ICR for updating business associate agreements in the existing information collections in Table 1.

**Burden Hours for Health Plan Sponsors' Compliance with Safeguards**

Table 3. This table shows burden hours for health plan sponsors' compliance as a result of the proposed rule.

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours |
|---|---|---|---|---|---|---|
| 164.308 | Risk Analysis—Documentation | 742,411 | 1 | 742,411 | 5 | 3,712,055 |
| 164.308 | Information System Activity Review—Documentation | 742,411 | 12 | 8,908,932 | 0.75 | 6,681,699 |
| 164.308 | Ongoing Education | 742,411 | 12 | 8,908,932 | 0.17 | 1,484,822 |
| 164.308 | Security Incidents (Other than Breaches) —Documentation | 742,411 | 12 | 8,908,932 | 2 | 17,817,864 |
| 164.308 | Contingency Plan—Testing and Revision | 742,411 | 1 | 742,411 | 2 | 1,484,822 |
| 164.308 | Contingency Plan—Criticality Analysis | 742,411 | 1 | 742,411 | 0.5 | 371,206 |
| 164.308 | Notification of Workforce Members' Termination of Access to ePHI | 742,411 | 1 | 742,411 | 0.25 | 185,603 |
| 164.308<br>164.312<br>164.314 | Maintenance Records | 742,411 | 12 | 8,908,932 | 0.5 | 4,454,466 |

| Section | Type of Respondent | Number of Respondents | Number of Responses per Respondent | Total Responses | Average Burden hours per Response[a] | Total Burden Hours |
|---|---|---|---|---|---|---|
| 164.312 | Multi-factor Authentication | 742,411 | 1 | 742,411 | 1.5 | 1,113,617 |
| 164.312 | Configuration Management | 742,411 | 1 | 742,411 | 0.5 | 371,206 |
| 164.312 | Penetration Testing | 742,411 | 1 | 742,411 | 2 | 1,484,822 |
| 164.314 | Notification of Contingency Plan Activation | 742,411 | 1 | 742,411 | 0.17 | 123,735 |
| **TOTAL** | | | | **41,575,016** | | **39,285,915** |

a. The figures in this column are averages based on a range. Small health plan sponsors may require fewer hours to conduct certain compliance activities, particularly those required by the Security Rule, while large health plan sponsors may spend more hours than those provided here because of their size and complexity.

## 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 for Regulated Entities | 1,140,446,641 | 848,076,471 |
| Table 2. Burden Hours of New Information Collections for Regulated Entities | 20,541,207 | 37,781,637 |
| Table 3. Burden Hours of Health Plan Sponsors' Compliance | 41,575,016 | 39,285,915 |
| **Total for the HIPAA Rules** | **1,202,562,864** | **925,144,023** |

**12B. Estimated Annual Burden Costs**

The total cost of this information collection, apart from capital costs, is approximately $109,085,104,674. These figures are based on hourly wages. Benefits are calculated by multiplying the base hourly wage rate by two.

**Updated Costs of Compliance for Regulated Entities with Existing Information Collections**

Table 5. This table 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 | 18,226,000 | $119.94[a] | $2,186,026,440 |
| 164.308 | Information System Activity Review —Documentation | 16,403,400 | $119.94 | $1,967,423,796 |
| 164.308 | Ongoing Education | 21,871,200 | $119.94 | $2,623,231,728 |
| 164.308 | Security Incidents (Other than Breaches)—Documentation | 473,876,000 | $119.94 | $56,836,687,440 |
| 164.308 | Contingency Plan—Testing and Revision | 14,580,800 | $119.94 | $1,748,821,152 |
| 164.308 | Contingency Plan—Criticality Analysis | 7,290,400 | $119.94 | $874,410,576 |
| 164.310 | Maintenance Records | 131,227,200 | $111.08[b] | |

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| | | | | $14,576,717,376 |
| 164.314 | Security Incidents—Business Associate Reporting of Non-breach Incidents to Covered Entities | 120,000,000 | $119.94 | $14,392,800,000 |
| 164.316 | Documentation—Review and Update | 10,935,600 | $119.94 | $1,311,615,864 |
| 164.404 | Individual Notice—Written and E-mail Notice— Drafting | 32,296 | $98.14[c] | $3,169,529 |
| 164.404 | Individual Notice—Written and E-mail Notice— Preparing and Documenting Notification | 32,296 | $46.10[d] | $1,488,846 |
| 164.404 | Individual Notice—Written and E-mail Notice— Processing and Sending | 336,038 | $46.10 | $15,491,340 |
| 164.404 | Individual Notice—Substitute Notice — Posting or Publishing | 2,950 | $104.64[e] | $308,688 |
| 164.404 | Individual Notice—Substitute Notice — Staffing Toll-free Number | 3,481 | $46.10 | $160,474 |
| 164.404 | Individual Notice—Substitute Notice — Individuals' Voluntary Burden to Call Toll-free Number for Information | 5,220 | $62.96[f] | $328,655 |
| 164.406 | Media Notice | 783 | $81.73[g] | $63,955 |
| 164.408 | Notice to Secretary— Notice for Breaches Affecting 500 or More Individuals | 783 | $81.73 | $63,955 |
| 164.408 | Notice to Secretary— Notice for Breaches Affecting Fewer than 500 Individuals | 63,966 | $46.10 | $2,948,833 |
| 164.410 | Business Associate Notice to Covered Entity—500 or More Individuals Affected | 1,000 | $129.28[h] | $129,280 |

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.410 | Business Associate Notice to Covered Entity—Less than 500 Individuals Affected | 9,320 | $129.28 | $1,204,890 |
| 164.414 | 500 or More Affected Individuals—Investigating and Documenting Breach | 31,300 | $129.28 | $4,046,464 |
| 164.414 | Less than 500 Affected Individuals—Investigating and Documenting Breach | 18,592 (for breaches affecting 10-499 | $129.28 | $2,403,574 |
| | | 246,568 (for breaches affecting <10 individuals) | $129.28 | $31,876,311 |
| 164.504 | Uses and Disclosures—Organizational Requirements | 68,550 | $98.14 | $6,727,497 |
| 164.508 | Uses and Disclosures for Which Individual Authorization is Required | 822,600 | $119.94 | $98,662,644 |
| 164.509 | Disclosures for Which Attestation is Required | 232,850 | $93.01[i] | $21,658,163 |
| 164.509 | Attestation Investigation Review | 1,300 | $169.68[j] | $220,584 |
| 164.509 | Attestation Requiring Additional Action | 975 | $129.28 | $126,048 |
| 164.512 | Uses and Disclosures for Research Purposes | 12,821 | $98.14 | $1,258,294 |
| 164.520 | Notice of Privacy Practices for Protected Health Information—Health Plans – Periodic Distribution of NPPs by Paper Mail | 625,000 | $46.10 | $28,812,500 |
| 164.520 | Notice of Privacy Practices for Protected Health Information—Health Plans – Periodic Distribution of NPPs by Electronic Mail | 417,500 | $46.10 | $19,246,750 |

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.520 | Notice of Privacy Practices for Protected Health Information—Health Care Providers—Dissemination and Acknowledgement | 30,650,000 | $98.14 | $3,007,991,000 |
| 164.522 | Rights to Request Privacy Protection for Protected Health Information | 2,000 | $98.14 | $196,280 |
| 164.524 | Access of Individuals to Protected Health Information—Copies of PHI | 30,750 | $98.14 | $3,017,805 |
| 164.526 | Amendment of Protected Health Information—Requests | 12,500 | $98.14 | $1,226,750 |
| 164.526 | Amendment of Protected Health Information—Denials | 4,167 | $98.14 | $408,917 |
| 164.528 | Accounting for Disclosures of Protected Health Information | 250 | $98.14 | $24,535 |
| **TOTAL** | | | | **$99,770,998,501[k]** |

a. The $119.94 wage, which includes $59.97 plus 100% for benefits, applies to the category “Information Security Analysts.”
b. The $111.08 wage, which includes $55.54 plus 100% for benefits, applies to the category “Management Analysts.”
c. The $98.14 wage, which includes $49.07 plus 100% for benefits, applies to the category “Healthcare Practitioners and Technical Occupations.”
d. The $46.10 wage, which includes $23.05 plus 100% for benefits, applies to the category “Office and Administrative Support Occupations.”
e. The $104.64 wage, which includes $52.32 plus 100% for benefits, applies to the category “Web and Digital Interface Designers.”
f. The $62.96 wage, which includes $31.48 plus 100% for benefits, applies to the category “All Occupations.”
g. The $81.73 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 ($153.30 per hour including benefits) and dividing the sum by the total number of burden hours.
h. The $129.28 wage, which includes $64.64 plus 100% for benefits, applies to the category “Medical and Health Services Manager.”
i. The $93.01 average cost per hour is derived by averaging the wages of the categories “Medical and Health Services Managers,” “Healthcare Practitioners and Technical Occupations,” and “Medical Records Specialists,” which includes $46.51 plus 100% for benefits.
j. The $169.68 wage, which includes $84.84 plus 100% for benefits, applies to the category “Lawyers.”
k. Total may not add up because of rounding.

## Costs of Compliance for Regulated Entities with New Information Collections

Table 6. This table shows the annual costs of complying with new burdens.

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.308 | Security Rule Compliance Audit | 3,645,200 | $119.94 | $437,205,288 |
| 164.308 | Business Associate Verification of Technical Safeguards | 2,000,000 | $119.94 | $239,880,000 |
| 164.308 | Covered Entity's Obtain Business Associate Compliance Verification | 411,300 | $119.94 | $49,331,322 |
| 164.308 | Business Associate Obtain Subcontractors' Compliance Verification | 83,333 | $119.94 | $9,995,000 |
| 164.308 | Notification of Workforce Members' Termination of Access to ePHI | 1,822,600 | $46.10 | $84,021,860 |
| 164.308 | Update Workforce Training | 3,645,200 | $69.20 | $252,247,840 |
| 164.308 | Update Business Associate Agreements | 1,822,600 | $169.68 | $309,258,768 |
| 164.312 | Multi-factor Authentication | 2,733,900 | $119.94 | $327,903,966 |
| 164.312 | Network Segmentation | 8,201,700 | $119.94 | $983,711,898 |
| 164.312 | Configuration Management | 697,698 | $119.94 | $83,681,898 |
| 164.312 | Penetration Testing | 5,467,800 | $119.94 | $655,807,932 |
| 164.314 | Notification of Contingency Plan Activation | 500,000 | $119.94 | $59,970,000 |
| 164.314 | Revise Health Plan Documents | 371,206 | $145.14[a] | $53,876,766 |
| 164.308, 164.310, 164.312 | Revise Policies and Procedures | 6,379,100 | $173.76 | $1,108,432,416 |
| **TOTAL** | | | | **$4,655,324,954[b]** |

a. The $145.14 wage, which includes $72.57 plus 100% for benefits, applies to the category "Compensation and Benefits Manager."
b. Total may not add up because of rounding.

## Health Plan Sponsors' Costs of Compliance with Safeguards

Table 7. This table shows the annual costs of health plan sponsors complying with administrative, physical, and technical safeguards.

| Section | Type of Respondent | Total Burden Hours | Hourly Wage | Total Respondent Costs |
|---|---|---|---|---|
| 164.308 | Risk Analysis—Documentation | 3,712,055 | $119.94 | $445,223,877 |
| 164.308 | Information System Activity Review—Documentation | 6,681,699 | $119.94 | $801,402,978 |
| 164.308 | Ongoing Education | 1,484,822 | $119.94 | $178,089,551 |
| 164.308 | Security Incidents (Other than Breaches)—Documentation | 17,817,864 | $119.94 | $2,137,074,608 |
| 164.308 | Contingency Plan—Testing and Revision | 1,484,822 | $119.94 | $178,089,551 |
| 164.308 | Contingency Plan—Criticality Analysis | 371,206 | $119.94 | $44,522,388 |
| 164.308 | Notification of Workforce Members' Termination of Access to ePHI | 185,603 | $46.10 | $8,556,287 |
| 164.308<br>164.312<br>164.314 | Maintenance Records | 4,454,466 | $111.08 | $494,802,083 |
| 164.312 | Multi-factor Authentication | 1,113,617 | $119.94 | $133,567,163 |
| 164.312 | Configuration Management | 371,206 | $119.94 | $44,522,388 |
| 164.312 | Penetration Testing | 1,484,822 | $119.94 | $178,089,551 |
| 164.314 | Notification of Contingency Plan Activation | 123,735 | $119.94 | $14,840,796 |
| **TOTAL** | | | | **$4,658,781,219**[a] |

a. Total may not add up because of rounding.

## 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 for Regulated Entities | $99,770,998,501 |
| Table 6. Costs of New Burdens for Regulated Entities | $4,655,324,954 |
| Table 7. Costs of Health Plan Sponsors' Compliance with Burdens | $4,658,781,219 |
| **TOTAL OF ALL HOURLY LABOR COSTS** [a] | **$109,085,104,674** |

a. Total may not add up because of rounding.

**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 are incurred by respondents for printing notices of privacy practices, and in certain cases, mailing the notices to the individual.

**Total Annual/Annualized Capital Costs**

Table 9.

| Section | Cost Elements | Number of Breaches | Cost per Breach | Total Cost |
|---|---|---|---|---|
| 164.404 | Individual Notice—Postage, Paper, and Envelopes | 64,592 | $263.95[a] | $17,049,295 |
| 164.404 | Individual Notice—Substitute Notice Media Posting | 2,950[b] | $480 | $1,416,000 |
| 164.404 | Individual Notice—Substitute Notice—Toll-Free Number | 2,950 | $64.95[c] | $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[d] |
| 164.520 | Postage and Envelope for Notice of Privacy Practices for Protected Health Information (health plans) | 15,000,000 | $.72 | $10,859,700[e] |
| 164.520 | Printing Notice of Privacy Practices for Protected Health Information (health care | 613,000,000 | $.18 | $107,642,800[f] |

| | | | | |
|---|---|---|---|---|
| | providers) | | | |
| **Total** | | | | **$163,499,411[g]** |

a. OCR again assumes that half of all affected individuals (half of 42,004,718 equals 21,002,359) would receive paper notification and half would receive notification by email. Therefore, on average, 325 individuals per breach would receive notification by mail. Further, OCR estimates that each mailed notice would 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.
b. The number of breaches requiring substitute notice equals all 626 large breaches and all 2,324 breaches affecting 10-499 individuals.
c. 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.
d. 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.
e. This number results from the following assumptions: 10% of 150 million notices (15,000,000) would 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.
f. This estimate includes 613 million notices with a combined cost for paper and printing of $.18 per notice.
g. Total may not add up because of 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 is borne by regulated entities. OCR does not produce or provide regulated entities with the required notifications, nor does it require regulated 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 separately 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 regulated entities that have experienced breaches affecting more than 500 individuals (referred to herein as "large breaches"). 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 decrease in the number of requests for exceptions from preemption of state law in the first year after the rule becomes effective, following a temporary increase as a result of previous changes to the Privacy Rule. This decrease would represent a return to the previous baseline of one request for exception from preemption of state law per year, at a cost to the Department of approximately $1,782. This includes a total of 14 burden hours to the Department for reviewing and responding to the request (10 hours for a GS-14/15 and 4 hours for a Senior Executive Service (SES) position).

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

The NPRM associated with this ICR proposes program changes since the previous information collection submission; thus, this information collection reflects new proposed requirements for regulated entities and group health plan sponsors. It does not create any modified burdens or quantifiable savings for individuals. The Department proposes to modify the Security Rule to strengthen the cybersecurity of individuals' ePHI by:

(1) Removing the distinction between "required" and "addressable" implementation specifications and making them all required with specific, limited exceptions.

(2) Requiring written documentation of all policies, procedures, plans, and analyses and documentation of the regulated entity's implementation of the Security Rule's standards.

(3) Updating definitions and revising implementation specifications to reflect changes in technology and terminology.

(4) Modifying the general rules for the Security Standards and the introductory language of the three categories of safeguards (*i.e.*, administrative, physical, and technical) to clarify that

implementation of the standards and implementation specifications is required throughout the enterprise.

(5) Aligning the standards and implementation specifications with widely accepted best practices in cybersecurity.

In addition to these changes, the Department added new burdens as a result of proposed program changes that would establish new requirements, as follows:

(1) For each regulated entity to conduct a Security Rule compliance audit.

(2) For each business associate (including each subcontractor) to provide verification of compliance with technical safeguards.

(3) For each regulated entity to obtain verification of business associates' and subcontractors' compliance with technical safeguards.

(5) For each regulated entity to provide notification to other regulated entities of workforce members' termination of access to ePHI.

(6) For each regulated entity to deploy multi-factor authentication.

(7) For each regulated entity to perform network segmentation.

(8) For approximately 76.56 percent of regulated entities to disable unused ports and remove extraneous software.

(9) For each regulated entity to conduct penetration testing.

(10) For each regulated entity to notify covered entities or business associates, as applicable, upon activation of a contingency plan.

(11) For each insurer and third-party administrator to update health plan documents.

(12) For each regulated entity to update the content of its cybersecurity awareness and Security Rule training program.

(13) For each regulated entity to update its policies and procedures.

(14) For each regulated entity to update business associate agreements.

(15) For each health plan sponsor that has access to ePHI to implement the Security Rule's administrative, physical, and technical safeguards in their relevant electronic information systems.

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 covered entities from 774,331 to 822,600.

**(2)** Updating hourly wage rates from 2022 to 2023 rates.

**(3)** Decreasing the number of respondents requesting exceptions to state law preemption under 45 CFR 160.204 from 27 to 1 to return to the previous baseline of 1 request per year.

**(4)** Decreasing the estimated hourly burden for a business associate to report security incidents (other than breaches) to a covered entity from 20 hours per monthly report to 10 hours per monthly report.

**(5)** Increased the estimated number of disclosures for research from approximately 147,000 to 153,857.

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 $107,492,846,352 to $109,248,604,085.

**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.