



DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

[Document Identifier: HHS-OS-0945-0003-60D]

Agency Information Collection Activities; Proposed Collection; Public Comment Request

AGENCY: Office of the Secretary.

ACTION: Notice.

SUMMARY: In compliance with section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995, the Office of the Secretary (OS), Department of Health and Human Services, announces plans to submit an Information Collection Request (ICR), described below, to the Office of Management and Budget (OMB). The ICR is for revision of the approved information collection assigned OMB control number #0945-0003, which expires on January 1, 2017. Prior to submitting that ICR to OMB, OS seeks comments from the public regarding the burden estimate, below, or any other aspect of the ICR.

DATES: Comments on the ICR must be received on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Submit your comments to Information.CollectionClearance@hhs.gov or by calling (202) 690-6162.

FOR FURTHER INFORMATION CONTACT: Information Collection Clearance staff, Information.CollectionClearance@hhs.gov or (202) 690-6162.

SUPPLEMENTARY INFORMATION: When submitting comments or requesting information, please include the document identifier HHS-OS-0945-0003-60D for reference.

Information Collection Request Title: HIPAA Privacy, Security, and Breach Notification Rules, and Supporting Regulations Contained in 45 CFR Parts 160 and 164

Abstract: This revision does not change any requirements of the HIPAA Privacy, Security, and Breach Notification Rules. Among other updates summarized below, the ICR requests to rename the information collection and incorporate into it the substance of two other information collections (#0945-0004, set to expire on May 31, 2016; and #0945-0001, expiring on September 30, 2016), which then would be discontinued. The ICR addresses the burden on regulated entities for compliance with the information collection requirements of the HIPAA Privacy, Security, and Breach Notification Rules; the voluntary burden on members of the public for obtaining information from covered entities regarding breaches of their protected health information; and the information collection burden on the Office for Civil Rights (OCR) associated with administering aspects of the HIPAA Breach Notification program. Combining the three existing information collections identified above will allow the regulated community, the public, and OCR to more easily view and track the estimated burdens associated with the HIPAA Rules that are administered and enforced by OCR. In addition to combining the ICRs, the proposed updates take into account our experience administering the Rules to more accurately reflect the burdens of compliance with the applicable regulatory requirements;

remove the estimated burden of initial compliance with the Omnibus HIPAA Final Rule, because we are well past the compliance dates; and incorporate increases in wages for the job categories that we expect to be involved in compliance activities.

Need and Proposed Use of the Information: The HIPAA Rules require covered entities, and in many respects their business associates, to protect the privacy and security of individually identifiable health information (called “protected health information” or “PHI”); fulfill individuals’ rights under HIPAA with respect to their health information; and provide notification in case of a breach of unsecured protected health information.

The information collections associated with these regulatory requirements include documenting and updating policies and procedures for ensuring the privacy and security of individuals’ health information, recording compliance activities, providing individuals with a notice of privacy practices and with access to their information upon request, and notifying affected individuals, the Secretary, and in some cases the media of a breach of protected health information.

Likely Respondents: HIPAA covered entities and business associates (required burden), and individual members of the public affected by breaches of their protected health information (voluntary burden)

Burden Statement: Burden in this context means the time expended by persons to generate, maintain, retain, disclose or provide the information requested. This includes the time needed to review instructions, to develop, acquire, install and utilize technology and systems for the purpose of collecting, validating and verifying information,

processing and maintaining information, and disclosing and providing information, to train personnel and to be able to respond to a collection of information, to search data sources, to complete and review the collection of information, and to transmit or otherwise disclose the information. The total annual burden hours estimated for this ICR are summarized in the table below.

Total Estimated Annualized Burden - Hours

Section	Type of Respondent	Number of Respondents	Number of Responses per Respondent	Average Burden hours per Response¹	Total Burden Hours
160.204	Process for Requesting Exception Determinations (states or persons)	1	1	16	16
164.308	Risk Analysis - Documentation	1,700,000 ²	1	10	17,000,000
164.308	Information System Activity Review –	1,700,000	12	.75	15,300,000

¹ 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.

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

	Documentation				
164.308	Security Reminders – Periodic Updates	1,700,000	12	1	20,400,000
164.308	Security Incidents (other than breaches) – Documentation	1,700,000	52	5	442,000,000
164.308	Contingency Plan – Testing and Revision	1,700,000	1	8	13,600,000
164.308	Contingency Plan – Criticality Analysis	1,700,000	1	4	6,800,000
164.310	Maintenance Records	1,700,000	12	6	122,400,000
164.314	Security Incidents – Business Associate reporting of incidents (other than breach) to Covered Entities	1,000,000	12	20	240,000,000
164.316	Documentation – Review and Update ³	1,700,000	1	6	10,200,000
164.404	Individual Notice—Written and E-mail Notice (drafting)	58,481 ⁴	1	.5	29,240
164.404	Individual Notice—Written and E-mail Notice (preparing and documenting notification)	58,481	1	.5	29,240

³ This element includes the burden of updating documentation in accordance with the evaluation required by 45 CFR 164.306. Therefore, we do not separately address the burden associated with the evaluation.

⁴ Total number of breach incidents in 2015.

164.404	Individual Notice—Written and E-mail Notice (processing and sending)	58,481	353 ⁵	.008	165,150
164.404	Individual Notice—Substitute Notice (posting or publishing)	2,746 ⁶	1	1	2,746
164.404	Individual Notice—Substitute Notice (staffing toll-free number)	2,746	1	5.75 ⁷	15,789
164.404	Individual Notice—Substitute Notice (individuals' voluntary burden to call toll-free number for information)	11,326,440 ⁸	1	.125 ⁹	1,415,805
164.406	Media Notice	267 ¹⁰	1	1.25	333

⁵ Average number of individuals affected per breach incident in 2015.

⁶ This number includes all 267 large breaches and all 2,479 breaches affecting 10-499 individuals. As we stated in the preamble to the Omnibus HIPAA Final Rule, although some breaches involving fewer than 10 individuals may require substitute notice, we believe the costs of providing such notice through alternative written means or by telephone is negligible.

⁷ We again assume that call center staff will spend 5 minutes per call, but now with an average of 4,124 individuals affected by breaches requiring substitute notice. Multiplying these figures results in 5.75 hours per breach. This estimate is much lower than the 46.26 hours per breach requiring substitute notice in our previous estimate, which we believe was the result of an arithmetic error. The estimate of 4,124 individuals being affected by breaches requiring substitute notice results from the assumption that the number of callers to the toll-free number will equal 10% of the sum of all individuals affected by large breaches (113,250,136) and 5% of individuals affected by small breaches (.05 x 285,413 = 14,270). We calculate $.10 * (113,250,136 + 14,270) = 11,326,440$.

⁸ 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.

⁹ This number includes 7.5 minutes for each individual who calls: an average of 2.5 minutes to wait on the line/decide to call back and 5 minutes for the call itself.

¹⁰ The total number of breaches affecting 500 or more individuals in 2015.

164.408	Notice to Secretary (notice for breaches affecting 500 or more individuals)	267	1	1.25	333
164.408	Notice to Secretary (notice for breaches affecting fewer than 500 individuals)	58,215 ¹¹	1	1	58,215
164.414	500 or More Affected Individuals (investigating and documenting breach)	267	1	50	13,350
164.414	Less than 500 Affected Individuals (investigating and documenting breach)	2,479 (breaches affecting 10-499 individuals)	1	8	19,832
		55,736 (breaches affecting <10 individuals)	1	4	222,944
164.504	Uses and Disclosures – Organizational Requirements	700,000	1	5/60	58,333
164.508	Uses and Disclosures for Which Individual authorization is required	700,000	1	1	700,000
164.512	Uses and Disclosures for	113,524 ¹²	1	5/60	9,460

¹¹ The total number of breaches affecting fewer than 500 individuals in 2015.

¹² The number of entities who use and disclose protected health information for research purposes.

	Research Purposes				
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by paper mail)	100,000,000 ¹³	1	0.25 minutes [1 hour per 240 notices]	416,667
164.520	Notice of Privacy Practices for Protected Health Information (health plans – periodic distribution of NPPs by electronic mail)	100,000,000	1	0.167 minutes [1 hour per 360 notices]	278,333
164.520	Notice of Privacy Practices for Protected Health Information (health care providers – dissemination and acknowledgement)	613,000,000 ¹⁴	1	3/60	30,650,000
164.522	Rights to Request Privacy Protection for Protected Health Information	20,000 ¹⁵	1	3/60	1,000

¹³ As in our previous submission, we assume that half of the approximately 200,000,000 individuals insured by covered health plans will receive the plan's NPP by paper mail, and half will receive the NPP by electronic mail.

¹⁴ We estimate that each year covered health care providers will have first-time visits with 613 million individuals, to whom the providers must give a NPP.

¹⁵ We assume covered entities address 20,000 requests for confidential communications or restrictions on disclosures per year.

164.524	Access of Individuals to Protected Health Information (disclosures)	200,000 ¹⁶	1	3/60	10,000
164.526	Amendment of Protected Health Information (requests)	150,000	1	5/60	12,500
164.526	Amendment of Protected Health Information (denials)	50,000	1	5/60	4,166
164.528	Accounting for Disclosures of Protected Health Information	5,000 ¹⁷	1	3/60	250
Total					921,813,702

OS specifically requests comments on (1) the necessity and utility of the proposed information collection for the proper performance of the agency's functions, (2) the accuracy of the estimated burden, (3) ways to enhance the quality, utility, and clarity of the information to be collected, and (4) the use of automated collection techniques or other forms of information technology to minimize the information collection burden.

Terry S. Clark,
Asst Information Collection Clearance Officer.

¹⁶ We estimate that covered entities annually fulfill 200,000 requests from individuals for access to their protected health information.

¹⁷ We estimate that covered entities annually fulfill 5,000 requests from individuals for an accounting of disclosures of their protected health information.

[FR Doc. 2016-05961 Filed: 3/16/2016 8:45 am; Publication Date: 3/17/2016]