Supporting Statement for Electronic Security Standards for Privacy of Individually Identifiable Health Information and Supporting Regulations Contained in 45 CFR Part 164

A. Justification

1. Circumstances Making the Collection of Information Necessary

The ICR is for renewal of the approved information collection assigned OMB control number 0945-0004, scheduled to expire on May 31, 2016. The Office for Civil Rights (OCR) requests approval to extend this collection without change while OMB reviews our request to incorporate the burdens of compliance with the Security Rule into another existing ICR (OMB #0945-0003, for the HIPAA Privacy Rule and Supporting Regulations), which is being revised to better reflect our experience in administering and enforcing the HIPAA Rules. This ICR extends the existing approved information collection for applicable compliance activities associated with the HIPAA Security Rule. When the revised ICR with OMB #0945-0003 is approved, we will request that this ICR (OMB# 0945-0004) be discontinued.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) and its implementing regulations at 45 CFR Part 164, the HIPAA Security Rule, require covered entities (health plans, health care clearinghouses, and certain health care providers) to maintain strong protections for the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit. As required under title II, subtitle F, sections 261 through 264 of HIPAA, the Department of Health and Human Services adopted standards to secure electronic protected health information while in the custody of entities covered by HIPAA (covered entities) as well as in transit between covered entities and from covered entities to others. The standards adopted in the HIPAA Security Rule require the covered entities to maintain reasonable and appropriate administrative, physical and technical safeguards to ensure the integrity, availability and confidentiality of the information and to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information. These safeguards must also otherwise ensure compliance with the statute by the workforce members of the covered entities.

2. Purpose and Use of Information Collection

The information collected is used test the validity of complaints against covered entities and to verify the compliance of covered entities with the provisions of the HIPAA Security Rule.

3. Use of Improved Information Technology and Burden Reduction

The HIPAA Security Rule allows the information collected to be maintained electronically.

4. Efforts to Identify Duplication and Use of Similar Information

The requirements of the HIPAA Security Rule do not duplicate those of any other federal regulation.

5. Impact on Small Businesses or Other Small Entities

The HIPAA Security Rule does impact small businesses. However, the Security Rule requirements are both scalable and technically flexible. In addition, many of the implementation specifications are "addressable," meaning that an entity decides whether certain specifications are reasonable and appropriate security measures to apply within its particular security framework. This gives small businesses the opportunity to use their risk assessment to determine which measures are already in place, which are of particular importance to the entity, what the costs are, and which measures should be implemented. Documentation of such decisions is required.

6. Consequences of Less Frequent Collection

Under the HIPAA Privacy and Security Rules, the frequency of collection is a function of activity by covered entities and business associates and the policies and procedures that they establish for complying with the Rules, and of the need for the Department to examine the entities' policies and procedures for compliance and enforcement purposes, such as to evaluate a complaint against a covered entity or business associate.

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

The 60-day Federal Register notice published on March 15, 2016 (81 FR 13806). No public comments were received. The 30-day Federal Register Notice published on May 19, 2016 (81 FR 31645).

9. Explanation of Any Payment/Gift to Respondents

There are no payments or gifts to the respondents.

10. Assurance of Confidentiality Provided to Respondents

The HIPAA Security Rule complies with the Privacy Act of 1974 (5SUC 552a) and the Freedom of Information Act (5 CFR 552) with respect to information provided to OCR.

11. Justification for Sensitive Questions

The HIPAA Security Rule does not require that sensitive questions be asked.

12. Estimates of Annualized Burden Hours (Total Hours & Wages)

The estimates and explanations below are unchanged from the previously approved information collection. As explained above, we have submitted a revised information collection request under a different number (0945-0003) that incorporates updated estimated Security Rule burdens (including for the requirements addressed below). We request that this existing information collection (0945-0004) be extended only until the revised, comprehensive information collection is approved.

The overall total for respondents to comply with the information collection requirements of the HIPAA Security Rule is 536,743 burden hours.

12A. Estimated Annualized Burden Hours

Section within 45 CFR 164	Response Type	Number of Respondents	Number of Responses per Respondent	Average Burden hours per Response	Total Burden Hours
306	Justification	75,000	3	15/60	56,250
308	Security incident report	50	1	8	400
308	Contingency plan	60,000	1	8	480,000
310	Physical safeguard policies and procedures	500	1	10/60	83
314	Problem reports	10	1	1	10
Total					**536,743**

12B. Estimated Annualized Burden Costs
There are no annualized costs estimated for the HIPAA Security Rule.

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

There are no capital costs associated with this information collection.

14. Annualized Cost to Federal Government

The Security Rule requires covered entities and business associates to record and maintain information in order to comply with the Rule's requirements. However, OCR does not produce the forms on which the information is recorded by the entities. There is thus no cost to the federal government for this portion of the information collection.

15. Explanation for Program Changes or Adjustments

Changes have been made to the total burden hour estimates in this supporting statement; due to an error in the previously approved ICR (for reinstatement and transfer of the ICR from CMS/OESS to OCR), the ROCIS table and supporting statement for this ICR did not match.

As noted above, to better reflect our experience, we make adjustments to the estimated burden of compliance with the Security Rule in the new, consolidated ICR (0945-0003), which we will submit shortly for review.

16. Plans for Tabulation and Publication and Project Time Schedule
Not applicable to the HIPAA Security Rule.

17. Reason(s) Display of OMB Expiration Date is Inappropriate
OCR has no concern displaying the OMB expiration date.

18. Exceptions to Certification for Paperwork Reduction Act Submissions
There are no exceptions to the certification.

B. Collection of Information Employing Statistical Methods
Not applicable. The information collection required by the HIPAA Security Rule as described above in part A does not require nor lend itself to the application of statistical methods.