

**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**

This information collection request is for reinstatement and transfer of a previously approved information collection, formerly assigned OMB # 0938-0949. The information collection will be reinstated to the Centers for Medicare and Medicaid Services. Once reinstated, the information collection will transfer to the Office of Civil Rights (OCR) within the Department of Health and Human Services, receiving a new OMB control number in the process.

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 HIPAA.

**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. Some were given an extra year to comply with the final rule. The Security Rule requirements are both scalable and technically flexible. The number of required implementation specifications are minimal, providing greater flexibility and allowing focus on what needs to be done. The final rule also made many of the implementation specifications “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**

The information will only be collected if it is needed for enforcement purposes or to evaluate a complaint against a covered entity. Information must be prepared and available, but will only be collected as needed.

#### **7. Special Circumstances Relating to the Guidelines of 5 CFR 1320.5**

The documentation/paperwork would only be collected on an “as needed” basis. With respect to proprietary information, it is possible that covered entities would consider their policies, procedures, and decision documents proprietary. The Office of E-Health Standards and Services (OEHS) for Civil Rights (OCR) is responsible for enforcement, and therefore the review of the materials. The OCR will have procedures to protect the information and will not distribute it to any other agency, individual or organization, unless that entity is bound by a contract to review the information, and that contract includes appropriate confidentiality language.

#### **8. Comments in Response to the Federal Register Notice/Outside Consultation**

The 60-day Federal Register notice published on August 31, 2012.

This rule was first published in the Federal Register (63 FR 43242) as HCFA-0049-P on August 12, 1998. The final rule was published in the Federal Register (68 FR 8334) as CMS-0049-F published on February 20, 2003.

#### **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 (5U.S.C. 552a) and the Freedom of Information Act (5 CFR 552).

#### **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)**

Because the HIPAA Security Rule has been in effect for several years, the burden hours estimate is based on past experience with this information collection and does not include

the initial burden of compliance. 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

| <b>Section within 45 CFR 164</b> | <b>Response Type</b>                       | <b>Number of Respondents</b> | <b>Number of Responses per Respondent</b> | <b>Average Burden hours per Response</b> | <b>Total Burden Hours</b> |
|----------------------------------|--|------------------------------|---|--|---------------------------|
| 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                        |
| <b>Total</b>                     |  |                              |   |  | <b>536,743</b>            |

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**

There are no estimated costs to the Federal Government for this information collection.

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

The total burden hours decreased because the original burden estimate included higher burden for initial compliance with the final rule. Since the final rule has been in effect for several years, the initial compliance burden is no longer applicable.

**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.