G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

B-324354

February 8, 2013

The Honorable Tom Harkin
Chairman
The Honorable Lamar Alexander
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Fred Upton
Chairman
The Honorable Henry A. Waxman
Ranking Member
Committee on Energy and Commerce
House of Representatives

Subject: *Department of Health and Human Services, Office of the Secretary: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*

Pursuant to section 801(a)(2)(A) of title 5, United States Code, this is our report on a major rule promulgated by the Department of Health and Human Services (HHS), Office of the Secretary entitled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules" (RIN: 0945-AA03). We received the rule on January 24, 2013. It was published in the *Federal Register* as a final rule on January 25, 2013. 78 Fed. Reg. 5566

The final rule was issued to modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement statutory amendments under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act" or "the Act") to strengthen the privacy and security protection for individuals' health information; modify the rule for Breach Notification for Unsecured Protected Health Information (Breach Notification Rule) under the HITECH Act to address public comment received on the interim final rule; modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic

information by implementing section 105 of title I of the Genetic Information Nondiscrimination Act of 2008 (GINA); and make certain other modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (the HIPAA Rules) to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities.

The rule has an effective date of March 26, 2013. Covered entities and business associates must comply with the applicable requirements of this final rule by September 23, 2013.

Enclosed is our assessment of HHS's compliance with the procedural steps required by section 801(a)(1)(B)(i) through (iv) of title 5 with respect to the rule. Our review of the procedural steps taken indicates that HHS complied with the applicable requirements.

If you have any questions about this report or wish to contact GAO officials responsible for the evaluation work relating to the subject matter of the rule, please contact Shirley A. Jones, Assistant General Counsel, at (202) 512-8156.

signed

Robert J. Cramer
Managing Associate General Counsel

Enclosure

cc: Ann Stallion
Program Manager
Department of Health and
Human Services

ENCLOSURE

REPORT UNDER 5 U.S.C. § 801(a)(2)(A) ON A MAJOR RULE
ISSUED BY THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES,
OFFICE OF THE SECRETARY
ENTITLED
"MODIFICATIONS TO THE HIPAA PRIVACY, SECURITY, ENFORCEMENT, AND BREACH NOTIFICATION RULES UNDER THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT AND THE GENETIC INFORMATION NONDISCRIMINATION ACT; OTHER MODIFICATIONS TO THE HIPAA RULES"
(RIN: 0945-AA03)

(i) Cost-benefit analysis

HHS performed a cost-benefit analysis in conjunction with the final rule. This final rule is anticipated to have an annual effect on the economy of $100 million or more, making it an economically significant rule under Executive Order 12,866. Accordingly, HHS prepared a Regulatory Impact Analysis that presents the estimated costs and benefits of the proposed rule. The total cost of compliance with the rule's provisions is estimated to be between $114 million and $225.4 million in the first year of implementation and approximately $14.5 million annually thereafter. Costs associated with the rule include: (1) costs to HIPAA covered entities of revising and distributing new notices of privacy practices to inform individuals of their rights and how their information is protected; (2) costs to covered entities related to compliance with breach notification requirements; (3) costs to a portion of business associates to bring their subcontracts into compliance with business associate agreement requirements; and (4) costs to a portion of business associates to achieve full compliance with the Security Rule.

HHS was not able to quantify the benefits of the rule due to lack of data and the impossibility of monetizing the value of individuals' privacy and dignity, which HHS believes will be enhanced by the strengthened privacy and security protections, expanded individual rights, and improved enforcement enabled by the rule. HHS also believes that some entities affected by the rule will realize cost savings as a result of provisions that simplify and streamline certain requirements, and increase flexibility, under the HIPAA Rules. However, HHS was unable to quantify such cost savings due to a lack of data.

(ii) Agency actions relevant to the Regulatory Flexibility Act, 5 U.S.C. §§ 603-605, 607, and 609

HHS expects that the cost of compliance with the final rule will not be significant for small entities. Nor is it expected that the cost of compliance will fall disproportionately on small entities. Although many of the covered entities and business associates affected by the rule are small entities, they do not bear a disproportionate cost burden compared to the other entities subject to the rule. With respect to small business associates, only the fraction of these entities that has not made a good faith effort to comply with existing requirements will experience additional costs under the rule. HHS certified that the final rule will not have a significant economic impact on a substantial number of small entities. Nonetheless, HHS considered and adopted several solutions for reducing the burden on small entities.

(iii) Agency actions relevant to sections 202-205 of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. §§ 1532-1535

HHS stated that it does not believe that the final rule will impose substantial direct compliance costs on state and local governments that are not required by statute, but that the estimated costs to private entities alone may exceed the $136 million threshold. HHS incorporated this analysis in the cost benefit analysis described above.

(iv) Other relevant information or requirements under acts and executive orders

Administrative Procedure Act, 5 U.S.C. §§ 551 et seq.

On July 14, 2010, HHS published a notice of proposed rulemaking (NPRM) to implement many of the remaining privacy, security, and enforcement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act and certain other modifications to the Health Insurance Portability and Accountability (HIPAA) Act of 1996 Rules in the *Federal Register*. 75 Fed. Reg. 40,868. HHS received about 300 comments on the NPRM. On October 30, 2009, HHS published an interim final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act. 74 Fed. Reg. 56,123. On August 24, 2009, HHS published an interim final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act that included a “harm” threshold, and under this final rule, a more objective standard has replaced the “harm” threshold. 74 Fed. Reg. 42,740. Further, on October 7, 2009, HHS published a proposed rule to strengthen the privacy protections for genetic information under the HIPAA Privacy Rule by implementing the protections for genetic information required by the Genetic Information Nondiscrimination Act of 2008 (GINA) and making related changes to

the rule. 74 Fed. Reg. 51,698. HHS received about 25 comments on the proposed rule. HHS merged these four rules into one omnibus final rule.

Paperwork Reduction Act, 44 U.S.C. §§ 3501-3520

The final rule contains information collection requirements subject to the Paperwork Reduction Act. The final rule describes changes from the information collection requirements related to reporting, recordkeeping, and third-party disclosures set out in the proposed and interim final rules. The information collection requirements described in this final rule have been submitted to the Office of Management and Budget for review and approval.

Statutory authorization for the rule

The final rule is authorized by sections 1171-1180 (Administrative Simplification) of the Social Security Act (42 U.S.C. §§ 1320d, 1320d-1, 1320d-2, 1320d-3, 1320d-4, 1320d-5, 1320d-6, 1320d-7, 1320d-8, 1320d-9), sections 262 (Administrative simplification) and 264 (Recommendations with respect to privacy of certain health information) of Pub. L. No. 104-191 (Health Insurance Portability and Accountability Act of 1996), section 105 (Privacy and confidentiality) of Pub. L. No. 110-233 (Genetic Information Nondiscrimination Act of 2008), sections 13400-13424 (HITECH Act) of Pub. L. 111-5 (American Recovery and Reinvestment Act of 2009), section 1104 (Administrative simplification) of Pub. L. No. 111-148 (Patient Protection and Affordable Care Act).

Executive Order No. 12,866 (Regulatory Planning and Review)

HHS determined that the final rule is economically significant under the Executive Order, and the rule was reviewed by the Office of Management and Budget.

Executive Order No. 13,132 (Federalism)

HHS has determined that the Privacy Rule's preemption provisions do not raise federalism issues. Further, HHS does not believe that the rule will impose substantial direct compliance costs on state and local governments that are not required by statute, and therefore does not have federalism implications.