May 11, 2010

The Honorable Nancy Pelosi
Speaker of the House of Representatives
H-209, The Capitol
Washington, D.C. 20510

Dear Mme Speaker:

I am pleased to transmit our Ninth *Annual Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act*. In compliance with Section 263, Subtitle F of Public Law 104-191, the report was developed by the National Committee on Vital and Health Statistics (NCVHS), the public advisory committee to the U.S. Department of Health and Human Services on health data, privacy, and health information policy, and covers the period January 1, 2007 through December 31, 2009. The Administrative Simplification provisions of HIPAA require the Secretary of Health and Human Services (HHS) to adopt a variety of standards to support electronic interchange for administrative and financial healthcare transactions, including standards for security and privacy to protect individually identifiable health information. The statute assigns expanded responsibilities to the National Committee on Vital and Health Statistics for advising the Secretary on health information privacy and on the adoption of health data standards. Among those responsibilities, the Committee is directed to submit an annual report to Congress on the status of implementation of the administrative simplification effort.

The previous (Eighth) Annual Report to Congress reflected on the HIPAA experience in light of the tenth anniversary of its enactment, offered some lessons learned, applauded the accomplishments under HIPAA, and reaffirmed the importance of the administrative simplification initiative to improving the efficiency and effectiveness of the U.S. healthcare system. The attached report also recognizes that while not all standards are identified or fully implemented, the promise of administrative simplification continues to be realized as the industry moves from "implementation" of the standards to "optimization" of work processes enabled by the standards. As noted in previous reports, however, the full economic benefits of Administrative Simplification will only be realized when all of the standards are in place; implementation activities and industry resource planning will be more effective when the entire suite of standards is finalized.

3311 Toledo Road • Room 2341 • Hyattsville, MD 20782 • (301) 458-4200 • Web site: www.ncvhs.hhs.gov

This reporting period saw significant changes to HIPAA privacy rule requirements in the enactment of the American Recovery and Reinvestment Act (ARRA, Public Law 111-5), and, in particular, Title XIII, called the Health Information Technology for Electronic and Clinical Health (HITECH) Act. Many of the regulations that will implement these changes are still being developed, but some were promulgated on a fast track to meet with statutory mandates.

We hope that you will find this report informative and useful. If you or your staff would like a briefing on any of our past or anticipated activities, please let me know.

We are committed to improvements in health information systems that will enhance the quality of healthcare, lower costs, and facilitate access to care in the U.S. We look forward to continued progress.

Sincerely,

/s/

Harry L. Reynolds, Jr.
Chairman, National Committee on Vital and Health Statistics

Enclosure

Identical letters to:

The Honorable Max Baucus
Chairman
Committee on Finance
219 Senate Dirksen Office Building
United States Senate
Washington, D.C. 20510

The Honorable Robert C. Byrd
President Pro Tempore
United States Senate
Washington, D.C. 20510

The Honorable Tom Larkin
Chairman
Committee on Health, Education, Labor and Pensions
428 Senate Dirksen Office Building
United States Senate
Washington, D.C. 20510

The Honorable Sandy Levin
Acting Chairman
Committee on Ways and Means
U.S. House of Representatives
1102 Longworth House Office Building
Washington, D.C. 20215

The Honorable George Miller
Chairman
Committee on Education and Labor
U.S. House of Representatives
2181 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Henry A. Waxman
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20215

Cc: The Honorable Kathleen Sebelius
HHS Data Council Co-Chairs:

NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

Administrative Simplification in Healthcare: January 1, 2007 – December 31, 2009

Ninth Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996

CONTENTS

I. Executive Summary

NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

Administrative Simplification in Healthcare: January 1, 2007 – December 31, 2009

Ninth Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996

This report describes the status of implementation of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The major purpose of the HIPAA Administrative Simplification provisions is to improve the efficiency and effectiveness of the nation's healthcare system, and, in particular, Medicare and Medicaid programs, by encouraging the electronic transmission of health information through the use of standards. The HIPAA information, privacy and security standards are required to be used by health plans, healthcare clearinghouses, and certain healthcare providers who transmit or maintain electronic health information.

Through HIPAA, Congress expanded the responsibilities of the National Committee on Vital and Health Statistics (NCVHS) that now include advising the Secretary of Health and Human Services (HHS) on the adoption of standards, monitoring their implementation, and reporting annually on progress. This report is the ninth report on implementation and covers the period January 1, 2007 through December 31, 2009.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 included a series of "administrative simplification" provisions requiring HHS to adopt national standards for certain electronic healthcare transactions and identifiers. By ensuring consistency throughout the industry, these standards are making it possible for health plans, healthcare clearinghouses, doctors, hospitals and other healthcare providers to process claims and other transactions electronically. The law also required the adoption of privacy and security standards in order to protect individually identifiable health information. HIPAA requires that "covered entities" e.g. health plans, healthcare clearinghouses, and those healthcare providers conducting electronic financial and administrative transactions (such as eligibility, referral authorizations, and claims) comply with the national standards. Other types of businesses may choose to use the standards, but the law does not mandate that they do so. For example, an employer may choose to use the standard transaction for enrollment and disenrollment, but is not required to use the standard because employers are not covered entities. In general, the law requires covered entities to comply with the standards within two years following adoption, except for small health plans, which have three years to come into compliance.

This reporting period saw significant changes to HIPAA privacy rule requirements in the enactment of the American Recovery and Reinvestment Act (ARRA, Public Law 111-5), and, in particular, Title XIII, called the Health Information Technology for Electronic and Clinical Health (HITECH) Act. Many of the regulations that will implement these changes are still being developed, but some were promulgated on a fast track to meet statutory mandates.

In response to these new requirements, NCVHS held hearings to collect information regarding how to interpret "meaningful use," a term of art in the ARRA that, when fully defined, will guide which healthcare providers are eligible for significant monetary incentives to adopt electronic health records. Additionally, NCVHS began collaborating with the two new Federal Advisory Committees created by the ARRA to advise the National Coordinator for Health Information Technology on issues of data stewardship, e-prescribing, and the nationwide health information network (NHIN).

Prior to enactment of ARRA, HHS was diligently working on the existing HIPAA requirements. HHS published final rules adopting updated versions of the Accredited Standards Committee (ASC) X12 and the National Council for Prescription Drug Programs (NCPDP) standards for electronic transactions and ICD-10-CM and ICD-10-PCS as HIPAA code sets; and adopted the National Provider Identifier (NPI) and implemented it through the National Plan and Provider Enumeration System (NPPES).

The NCVHS reaffirms the importance of the HIPAA administrative simplification provisions and continues its careful technical work on HIPAA. Much of NCVHS' advising has focused on the potential and the limits of health IT with respect to privacy, security, quality, standards, and population health. The pressing need for stewardship to permit multiple uses of health information is a growing emphasis and is reflected in an NCVHS Primer released in 2009. The major areas of work for NCVHS are information policy issues related to health IT and the NHIN, meaningful use of EHRs, health care

quality, data stewardship, population health data, privacy and confidentiality, security and standards. In 2009, NCVHS compiled all its landmark recommendations to the Department on privacy and confidentiality, between 2006 and 2008, and issued them as a single volume, to serve as a reference and resource for the field. NCVHS recommends that this volume become the "Roadmap" for privacy and confidentiality in electronic exchange of patient information.

If one single achievement is associated with NCVHS in recent years, it is probably the selection and recommendation of health IT standards that have now become the foundation for interoperability, care coordination, and the measurement of health care quality and outcomes. The HIPAA administrative simplification provisions had directed NCVHS to study and recommend standards for electronic patient medical record information (PMRI). NCVHS recognized this directive as new and strategic, because all of the other HIPAA standards were intended to support the reimbursement and statistical research processes, while the PMRI standards would need to support the patient care process in a real time clinically specific manner. These sets of standards have been adopted virtually unchanged as the foundation for the demonstration of meaningful use of HIT. NCVHS continues to advocate for a streamlined process for the development, adoption, and implementation of these standards.

II. Introduction

This report describes the status of implementation of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The administrative simplification provisions (title II, subtitle F of Pub. L. No. 104-191, adding a new title XI, part C, to the Social Security Act (42 U.S.C. § 1320d et seq.)) required the Secretary of Health and Human Services (HHS) to adopt standards for the electronic transmission of administrative and financial information throughout the healthcare system. By ensuring consistency throughout the industry, these national standards were expected to make it easier for health plans, healthcare clearinghouses, doctors, hospitals and other healthcare providers to process claims and other electronic transactions, and thereby to improve the efficiency and effectiveness of the healthcare system. The standards included transactions; code sets; unique identifiers of healthcare providers, health plans, employers, and individuals; and privacy and security standards to protect individually identifiable health information. Congress charged the National Committee on Vital and Health Statistics (NCVHS) to advise the Secretary of Health and Human Services on the adoption of standards, monitoring their implementation, and reporting on progress. This report is the ninth report on implementation and covers the period January 1, 2007 through December 31, 2009. Previous NCVHS reports to Congress about the progress of the implementation of administrative simplification may be found at the committee's web site, http://www.ncvhs.hhs.gov/.

NCVHS has examined the process of standards implementation and the issuance of rules to adopt standards. Now that most of the standards have been implemented, the NCVHS is identifying industry challenges and opportunities for improvement in the standards adoption and implementation processes.

To date, HHS has promulgated administrative simplification regulations on electronic healthcare transactions and code sets;[1] health information privacy;[2] unique

[1] General Provisions for Transactions, 45 C.F.R. pt. 162 pt. I; Code Sets, 45 C.F.R. pt. 162, subpt. J.
[2] Privacy of Individually Identifiable Health Information, 45 C.F.R. pts. 160 and 164.

identifiers for employers;[3] security of electronic protected health information;[4] unique identifiers for providers;[5] and enforcement procedures.[6]

Several rules under the original HIPAA legislation must still be published, including regulations for a unique health plan identifier, electronic healthcare claims attachments, and first report of injury. These are expected in the next few years, and NCVHS will support their publication through hearings and recommendations to the Secretary.

III. Specific Progress in HIPAA Standards Implementation

TRANSACTIONS AND CODE SET STANDARDS

Ongoing maintenance of standards and code sets. The final rule on transactions and code sets standards was issued on August 17, 2000, with a final compliance date of October 2003. When HHS published this first administrative simplification regulation, it recognized the need for the ongoing maintenance of the standards, and especially the need for the industry to identify, review and recommend changes to the standards themselves. The final regulation established an organization called a Designated Standards Maintenance Organization (DSMO) to receive and process requests for modifications to standards or for adopting new standards. The DSMO members include three data content committees and three standards development organizations. The DSMO regularly reports to the NCVHS Standards Subcommittee, sharing information about the types and number of change requests received, and the status of new versions for each standard transaction.

Based on a report from the DSMO in 2007 and testimony from healthcare providers, health plans, vendors, standards development organizations and others over a two day period, NCVHS submitted a number of recommendations to the Secretary proposing the adoption of updated versions of the existing standards and revisions to the standards adoption process for HIPAA transaction standards. Specifically, NCVHS recommended the adoption of NCPDP D.0 and its equivalent batch standard; the ASC X12N version 5010 transactions suite; and the NCPDP Medicaid Subrogation Standard version 3.0. To facilitate timely compliance, the subcommittee also recommended that the Secretary establish two levels of readiness for HIPAA implementation—level 1 for the internal testing and readiness of a covered entity, and level 2 for end-to-end testing with trading partners. Included in the recommendations to the Secretary were proposals for greater outreach to all constituents, and the compilation of best practices from the industry.

[3] Standard Unique Employer Identifier, 45 C.F.R. pt. 162, subpt. F.
[4] Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. pts. 160 and 164.
[5] Standard Unique Health Identifier for Healthcare Providers, 45 C.F.R. pt. 162, subpt. D.
[6] Enforcement Rule, 45 C.F.R. pt. 160, subpts. C, D, and E.

Regulation on claims attachments. HHS published an NPRM in September 2005, to adopt standards for exchanging supplemental claims information based on a request from a health plan, and a response from a provider. Extensive comments supporting the proposed rule were received, but the final rule has not been published pending decisions about the version to be adopted.

Published final rule adopting updated versions of the HIPAA standards (5010, D.0 and 3.0). In January 2009, HHS published a final rule adopting updated versions of all of the X12 and NCPDP standards for electronic transactions, allowing the industry to use the newer versions of the standards as soon as January 1, 2012. The rule also adopted a new standard, NCPDP Version 3.0, for Medicaid subrogation. This standard permits the industry to use a standard transaction for the process by which Medicaid agencies recoup payments for which another payer is the responsible party. All covered entities must comply by January 1, 2012, except small health plans, which have until January 1, 2013 to comply with the subrogation standard.

Published final rule adopting ICD-10 code sets. In January 2009, HHS also published the final rule adopting ICD-10-CM and ICD-10-PCS as HIPAA standards, replacing ICD-9-CM, Volumes 1, 2 and 3, which have been in use for 30 years. A comprehensive implementation plan has been developed for Medicare, as well as for CMS' other functions such as coverage policies, utilization management, and fraud and abuse prevention. All covered entities must comply by October 1, 2013.

IDENTIFIER STANDARDS

National Provider Identifier. HHS adopted a standard National Provider Identifier (NPI) to replace the legacy identifiers in 2004. In tandem, HHS created the National Plan and Provider Enumeration System (NPPES) to carry out the enumeration of all providers, and provide public access to the data. The compliance date for using the NPI was originally May 23, 2007. Providers began requesting NPIs in 2006, through the NPPES system, and in two years, more than 2 million numbers were disseminated. However, as entities began to re-program systems and build crosswalks between NPIs and legacy numbers, they discovered many complex challenges, threatening the deadline. Based on testimony to NCVHS, and its subsequent recommendations to the Secretary, the Department determined that the industry was not in a position to meet the compliance date. On April 2, 2007, the Department published guidance clarifying that covered entities making a good faith effort to comply with the NPI provisions could implement contingency plans to send or accept legacy provider numbers in order to maintain operations and cash flows for up to an additional twelve months. As a result of this feedback, the entire industry was required to be compliant by May 23, 2008. Healthcare providers, health plans, and clearinghouses creatively collaborated to ensure that this deadline was met.

Dissemination Policy for National Provider Identifier. In February 2007, CMS distributed a National Provider ID Data Dissemination Policy to notify covered entities which data elements (about a provider) would be available through the NPPES. The

Department received significant public comment from the industry objecting to the proposal and highlighting the risk to providers if certain data elements were made public. HHS provided an amnesty period to providers to remove sensitive information from their electronic files before the Department made the data available. The amnesty period ended in August 2007, and provider data became publically available on September 4. 2007.

National Health Plan Identifier. HIPAA requires HHS to establish a standard unique identifier for health plans, making it easier for healthcare providers to exchange transactions with the many health plans with which they conduct business. The publication date for this rule remains under discussion at HHS.

Unique Personal Identifier**.** HIPAA requires HHS to develop a unique personal identifier for every individual patient in the country to improve processing and recordkeeping in healthcare systems and transactions. Members of Congress have since expressed strong reservations about the appropriateness of creating a new identifier for individuals that might be perceived as a "universal identifier," and since 1999, the Congress has prohibited expending funds for its development in HHS' appropriations legislation. As a consequence, HHS has postponed development of such a standard indefinitely.

PRIVACY STANDARDS

Ongoing maintenance of privacy standards. The regulation on privacy standards, commonly called the Privacy Rule, was originally published on December 28, 2000. On August 14, 2002, prior to its implementation date, modifications to the Privacy Rule were adopted to address a number of workability issues. The Privacy Rule imposes obligations on covered entities to provide notices of their privacy practices and to use and disclose individually identifiable health information only as permitted or required by the Rule. The Privacy Rule also grants certain rights to individuals with respect to their information held by the covered entity, such as the right to review and obtain copies of their records, to correct or amend their records, and to obtain an accounting for certain disclosures of their information by the covered entity. Most covered entities were required to comply with the privacy rule by April 14, 2003, and small health plans were required to comply by April 14, 2004. NCVHS continues to monitor privacy issues by holding periodic hearings and making recommendations to the Secretary about the Privacy Rule.[7]

Harmonizing FERPA and HIPAA. Through a series of hearings in 2006 and 2007, NCVHS focused on improving the interaction of the Family Education Rights and Privacy Act (FERPA) and the HIPAA Privacy Rule. Building on past recommendations, this letter focused on three areas: disclosure of health information by educational entities; privacy and security of health information held by educational entities; and seeking clarification of when FERPA applies and when HIPAA applies, especially in the context of student employment. Since FERPA was enacted at a time prior to mainstreaming

[7] Note a report dated July 1, 2009 and a letter dated September 28, 2009 to the secretary available at http://ncvhs.hhs.gov/privacyreport0608.pdf and http://ncvhs.hhs.gov/090928lt.pdf respectively.

students with physical, developmental, behavioral and mental health conditions, NCVHS recommended HHS work with the Department of Education, which has oversight responsibility for FERPA, to improve the interaction of FERPA and the HIPAA Privacy Rule.

In November 2008, the Departments of Education and Health and Human Services published Joint Guidance on the Application of FERPA and HIPAA to Student Health Records. The purpose of this guidance was to explain the relationship between the two laws and to address apparent confusion on the part of school administrators, health care professionals, and others as to how these two laws apply to records maintained on students. In the wake of the tragedy at Virginia Tech, the guidance also addressed certain disclosures that are allowed without consent or authorization under both laws, especially those related to health and safety emergency situations. The Departments of Education and Health and Human Services are committed to a continuing dialogue with school officials and other professionals on these important matters affecting the safety and security of our nation's schools.

The Genetic Information Nondiscrimination Act of 2008 (GINA). In addition to prohibiting discrimination on the basis of genetic information in both the health insurance and employment arenas, GINA required amendments to the Privacy Rule to prohibit the use or disclosure of genetic information by health plans for underwriting purposes. On October 1, 2009, the Office for Civil Rights issued a notice of proposed rulemaking to impose this requirement on HIPAA covered health plans. Following analysis of the public comment, a final rule is expected to be issued in 2010.

Breach Notification Requirements. On August 24, 2009, OCR issued an interim final regulation implementing the new breach notification requirements from the HITECH Act of 2009.[8] HIPAA covered entities that experience a breach of protected health information are required to provide individuals affected by the breach with written notice, and if the breach affects 500 or more individuals to contemporaneously notify the Secretary and the media. The new breach notification requirements went into effect on September 23, 2009. Although issued as an interim final rule, public comment was accepted on these new requirements and a final regulation addressing those comments is expected in 2010.

SECURITY STANDARDS

Ongoing maintenance of security standards for electronic protected health information. The final rule for security standards was published in February 2003. Commonly known as the Security Rule, these regulations require covered entities to protect the confidentiality, integrity, and availability of electronic protected health information through administrative, physical and technical safeguards. Among the many requirements of the Security Rule, covered entities must perform a risk assessment and implement appropriate security measures to manage the risks to their electronic

[8] Breach Notification, 45 C.F.R., pt. 164, subpt. D.

information systems. Entities must have technical access and audit controls, physical safeguards to limit access to facilities and workstations and controls specific to portable media and devices containing electronic protected health information. The compliance date for most covered entities was April 21, 2005, and for small health plans, April 21, 2006.

Re-assignment of Security Rule administration and enforcement to OCR. In the original delegations of authority for HIPAA in October 2003, the Secretary delegated to the CMS administrator responsibility for transactions, code sets, identifiers and security, while responsibility for privacy was delegated to the Director of OCR. On July 27, 2009, Secretary Sebelius delegated the administration and enforcement of the HIPAA Security Rule to OCR. This action improves HHS' ability to protect individuals' health information by combining the authority of the Security and the Privacy Rules into one office. Additionally, Congress mandated improved enforcement of these rules in the 2009 HITECH provisions in ARRA. Privacy and security are reasonably and logically intertwined since both address the protection of health information in either electronic or paper form. Combining the enforcement authority into one agency within HHS eliminates the duplication of resource efforts and increases the efficiency of the investigations. Moreover, combining the administration of the Security Rule and the Privacy Rule supports the healthcare industry's shift to the increased adoption of electronic health records and electronic transmission of health information. The transition of authority for the administration and enforcement of the Security Rule was seamless and without interruption of any complaints filed prior to the transition and still under active investigation.

ENFORCEMENT

Ongoing maintenance of the Enforcement Rule. The Enforcement Rule for the Administrative Simplification provisions under HIPAA was published on February 16, 2006. The Enforcement Rule established a uniform set of procedures for any determination of compliance with or enforcement of HIPAA standards, including transactions and code sets, identifiers, privacy, and security. The Rule identifies covered entity and Departmental responsibilities for the conduct of investigations and compliance reviews, for the imposition of civil money penalties, and for hearing procedures if the review of a penalty is sought before the Departmental Appeals Board.

On October 29, 2009, the Department published an interim final rule to conform the civil money penalty and related provisions of the Enforcement Rule to the statutory changes enacted as part of the HITECH Act. Prior to the HITECH Act, the Secretary could not impose a penalty of more than $100 for each violation or $25,000 for all identical violations of the same provision within a calendar year. Section 13410(d) of the HITECH Act strengthened the civil money penalty scheme by establishing tiered ranges of increasing *minimum* penalty amounts. For example, for violations occurring after the date of enactment (February 17, 2009), where the entity did not know and could not have known of the violation, the minimum civil money penalty is $100 for each violation. For knowing violations, the minimum penalty increases to $1,000 for each violation; and for

violations due to the entity's willful neglect, the minimum penalty is $10,000 if promptly corrected or $50,000 if not corrected. For each tier, there is also a maximum penalty amount of $50,000 for each violation and an annual cap on multiple violations of the same provision of $1.5 million.

Transactions, Code Sets and Identifiers. As of December 2009, CMS had received 635 complaints alleging non-compliance with the Transactions and Code Sets (TCS) and NPI rules. Complaints included objections ranging from the failure of covered entities to accept compliant transactions to their failure to use updated versions of the code sets. CMS required the non-compliant entities to submit and implement corrective action plans, which CMS monitored. To date, CMS has not identified any instances of willful noncompliance, and, therefore, has not levied any financial penalties. NCVHS and CMS have been made aware that some parties are unwilling to file a complaint for fear of retribution. Despite public assurances to the contrary, the Committee believes that a number of noncompliant entities remain unidentified. CMS will continue to encourage entities to submit complaints. In 2009, CMS released a Request for Information (RFI) to solicit industry input on how compliance reviews could be conducted to evaluate compliance across the industry nationwide. Input from the responses will be evaluated to determine possible next steps.

Privacy. As of December 2009, OCR had received 48,768 complaints alleging non-compliance with the Privacy Rule. Of these complaints, OCR was able to resolve 28,221 cases without investigation. These administrative closures generally reflect the lack of jurisdiction, a defect or abandonment of the complaint, or the alleged activity does not constitute a violation of the Privacy Rule. Since April 2003, OCR has investigated and resolved over 9,854 complaints by requiring changes in privacy practices and other corrective actions by the covered entity. The corrective actions obtained by OCR have resulted in systemic change that affects all individuals served by the entity. An additional 5,047 cases were closed after the investigation found no violation had occurred. In July 2008, OCR together with CMS, entered into the first Resolution Agreement with Seattle-based Providence Health and Services, stemming from the loss of electronic backup media and laptop computers containing the protected health information of over 386,000 patients. In the Agreement, Providence agreed to pay $100,000 and implement corrective actions to ensure appropriate safeguards of electronic information against loss or theft. In January 2009, OCR entered into its second Resolution Agreement with CVS Pharmacy, Inc. to settle potential violations of the Privacy Rule. In the Agreement, CVS agreed to pay $2.25 million and implement corrective actions to ensure that it will appropriately dispose of protected health information, such as labels from prescription bottles and old prescriptions. In a coordinated action, CVS Caremark Corporation, the parent company of the pharmacy chain, also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act.

Security. Through July 27, 2009, CMS was responsible for enforcement of the Security Rule. Since its inception in 2005, fewer than 300 complaints were submitted, and most of those involved a concomitant allegation of a privacy violation (e.g. an employee looked at a colleague's data on the hospital's medical record system, but such

access was inappropriate to his or her job function, a stolen laptop with patient data). Therefore, many complaints were handled jointly between CMS and OCR. No cases of willful noncompliance were found. In most cases, poor judgment and human error were at the core of the incidents. During this time, the Department did not seek any civil money penalties for alleged security rule violations, but, as noted above, in a joint action with OCR, CMS entered into its first Resolution Agreement with Providence Health & Services, in which Providence agreed to pay $100,000 and undertake significant corrective actions to resolve allegations of inadequate safeguards of electronic media in violation of the Security Rule (stolen lap top computers).

CMS on-site security reviews. In 2008 and 2009, under its authority to conduct compliance reviews of covered entities, CMS launched a program for on-site reviews of several organizations. This program was in effect until July 2009, when enforcement of the Security Rule was transferred to OCR. During the two year program, CMS conducted more than 15 compliance reviews with findings ranging from the confirmation of solid security programs to missing policies, inadequate firewalls or insufficient workforce training. All entities cooperated fully and implemented corrective action plans to meet the identified deficits. Based on these reviews, CMS posted de-identified case examples on its website to serve as educational resources to benefit other covered entities.

Re-assignment of Enforcement of Security Rule to OCR. Following the July 27, 2009, delegation for the administration and enforcement of the HIPAA Security Rule to OCR, action continued without interruption on open complaints filed prior to the transition. Since taking over responsibility for Security Rule enforcement, OCR has received 16 new complaints and has closed 16 existing complaints. As of December 2009, there were approximately 95 complaints and/or compliance reviews that were actively being investigated.

HHS OUTREACH ACTIVITIES TO THE PRIVATE SECTOR ABOUT HIPAA

NCVHS has recommended that HHS provide information and guidance about HIPAA to the private sector, thereby, assisting in the industry's understanding of the various HIPAA regulations. HIPAA outreach strategies successfully deployed by CMS and OCR include a variety of efforts and activities such as creating user-friendly web sites, making numerous presentations to a broad range of audiences, posting updates to frequently asked "questions and answers," and making help desk support readily available. Increasingly, outreach materials specifically related to HIPAA privacy have been produced in collaboration with other Departments and agencies within HHS, such as the joint guidance with the Department of Education related to FERPA and HIPAA. Other examples include addressing privacy issues related to the Surgeon General's release of an Internet-based family health history tool in January 2009; HIPAA Privacy guidance for communications to friends, family, and others involved in a patient's care developed in conjunction with CMS in September 2008; and a series of technical assistance materials addressing how the Privacy Rule can facilitate electronic exchanges of data, the provision of electronic access to patient information, and protection of

information in Personal Health Records, all developed in December 2008 in conjunction with ONC's Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. During various hearings, testifiers have confirmed the effectiveness of these strategies and continue to ask for them as new regulations are enacted. CMS and OCR are to be commended for these valuable outreach activities.

STANDARDS ADOPTION PROCESS

In 2008 NCVHS received testimony from the industry about the rule-making process, described as too slow and cumbersome for updating the HIPAA transactions and code set standards. The process, beginning with the creation and approval of the standard, NCVHS hearings to recommend adoption of the standard, Secretary's concurrence to adopt the standard, publication of a proposed rule, followed by a comment period, publication of a final rule, and ultimate implementation of the standard, takes several years and necessarily slows the industry's ability to use newer versions of standards. This process hampers the industry's ability to keep pace with emerging business and technical needs, especially in an environment encouraging the rapid adoption and use of HIT systems. The industry also acknowledged an equally cumbersome standards development process, which requires similar publishing and vetting in the private sector but often on different time schedules than the federal rule-making process. The industry reported the different pathways create an uncertain environment when trying to develop proper solutions to accommodate the changes in the standards. NCVHS recommended where feasible, that voluntary adoption of the standards that minimally retain the full functionality of the previous adopted version should be permitted, thus, providing flexibility for the use of newer versions of the standards between willing trading partners. NCVHS also recommended that the Department explore ways to facilitate more expedient adoption and implementation of HIPAA standards. NCVHS suggested that HHS conduct an in-depth evaluation of the statutory and regulatory requirements, such as those under the Administrative Procedures Act (APA), to determine whether regulatory changes permitting the voluntary adoption of backward compatibility updates of standards could be implemented.

IV. Impact of HIPAA Legislation

NCVHS continues to serve as the Department's primary liaison with the private sector to obtain the views, perspectives, and concerns of the interested and affected parties, as well as their input and advice, on issues of health information policy, health data and statistics. NCVHS' full committee meets four times per year, and subcommittees and workgroups hold hearings and meetings throughout the year. Twenty-eight such hearings were held over the three year period of this report, many of which were relevant to HIPAA administrative simplification. From January 1, 2007 through December 31, 2009, the focus of NCVHS public hearings and subcommittee deliberations about HIPAA administrative simplification covered topics focusing on health data quality, population health, standards, privacy, confidentiality and security. Historically, and as part of the mandate by the HIPAA legislation, NCVHS also held hearings and made

recommendations to the Secretary about Patient Medical Record Information (PRMI)[9] issues related to the adoption of uniform data standards and the electronic exchange of such information. The PMRI work has been vital in bridging the gap between the administrative and clinical data exchange environments.

Congress, agencies within the Department and the Office of the National Coordinator (ONC) have called upon NCVHS to make recommendations in a number of additional areas. The Medicare Prescription Drug, Improvement and Modernization Act of 2003 directed NCVHS to develop recommendations for uniform standards to enable electronic prescribing in ambulatory care. NCVHS continued to discharge this responsibility during this reporting period with three letters. In 2007, in response to a request from ONC, NCVHS recommended a framework for secondary uses of electronically collected and transmitted health data. Then, the National Coordinator for the Office of Health Information Technology and CMS requested the expertise of the Committee after the passage of the American Recovery and Reinvestment Act of 2009 (ARRA), specific to Title XIII, the Health Information Technology for Economic and Clinical Act (HITECH) and Title IV, Medicare and Medicaid HIT. Both Title provisions provided an opportunity for NCVHS to address necessary specifications for the Nationwide Health Information Network (NHIN) and meaningful use of HIT. The following section details the NCVHS activities that support the healthcare industry's move forward for adopting, implementing and meaningfully using a nationwide information infrastructure through the standard and secure exchange of all health data.

DATA STEWARDSHIP

NCVHS developed recommendations about data stewardship over a seven month period of hearings in 2007 at the request of ONC. The hearings addressed benefits, sensitivities, obligations, and protections of data uses for quality measures, reporting quality improvement; research; and other purposes beneficial to the health of Americans and the healthcare delivery system. The nine recommendations called attention to the need for a transformation to enhanced protections for all uses of health data by all users, independent of HIPAA. Data stewardship includes accountability and chain of trust, transparency, individual participation, de-identification, security safeguards and controls, data quality and integrity, and oversight of data uses. The original NCVHS report, *Enhanced Protections for the Uses of Health Data: a Stewardship Framework*, dated December 22, 2007 was updated and posted to the NCVHS website April 24, 2008 with an additional *Health Data Stewardship: an NCVHS Primer* added in September, 2009.

REGULATIONS FOR E-PRESCRIBING

NCVHS continued its activities throughout 2008-2009 to evaluate and promote standards and regulations necessary for practitioners to employ electronic prescribing under Medicare Part D. In May 2008, the Committee issued recommendations about e-prescribing standards for long-term care (LTC) to the Secretary, proposing that voluntary

[9] The term "PMRI," which was specifically included in the HIPAA legislation refers to health information beyond claims-related data and was anticipated as a future need in the exchange of clinical data.

adoption allow for backward compatibility of the NCPDP Script version 10.5, which is used in LTC settings. The Committee acknowledged that proposed regulations issued by the Department of Justice on controlled substances would have negative consequences for the adoption of e-prescribing and recommended that HHS work with the Drug Enforcement Administration (DEA) on alternative solutions to arrive at a balanced, risk-based approach to assure security and functionality within clinical practice.[10] Finally, the Committee recommended that the Department adopt the next version of NCPDP (10.6) under a streamlined process continuing to allow for backward compatibility.[11]

NATIONWIDE HEALTH INFORMATION NETWORK

In June 2007 and February 2008, in response to an earlier request from ONC, the Committee made recommendations about the privacy and security of information that might be transmitted over the Nationwide Health Information Network (NHIN). The June 2007 hearings were designed to learn about various businesses that use health information in their day-to-day operations, but which are not covered by the HIPAA Privacy Rule. These include life insurers, insurance regulators, human resource professionals, some occupational health physicians, financial institutions, primary and secondary schools, colleges, and healthcare providers that do not conduct electronic transactions (e.g. those that do not accept any insurance). The Committee recommended that the federal government adopt privacy laws and regulations covering personally identifiable information wherever it may be held. This would help assure the public that the NHIN will be trustworthy because if information is created in electronic form it may easily find its way into the computer systems of many non-covered entities.[12]

Another NCVHS letter in 2008 made recommendations about individual control of sensitive health information accessible through the NHIN for the purposes of treatment. NCVHS made five recommendations (including twelve subparts) with the general theme for the need to adopt a policy (for the NHIN) to allow individuals to have limited but uniform control over the disclosures of specific categories of sensitive health information for treatment purposes. The Committee expressed its concern for the protection of patients' legitimate concern about privacy and confidentiality, the need to foster trust and encourage participation in the NHIN to improve patient care, and the desire to protect the integrity of the healthcare system.[13]

MEANINGFUL USE OF HEALTH INFORMATION TECHNOLOGY

At the request of the new National Coordinator for Health Information Technology and CMS, NCVHS held a 2-day hearing in the spring of 2009 to learn from the broad spectrum of stakeholders their views of "meaningful use" of health information

[10] Note a letter dated September 24, 2008 to the secretary available at http://www.ncvhs.hhs.gov/080924lt.pdf
[11] Note a letter dated July 1, 2009 to the secretary available at http://ncvhs.hhs.gov/090701lt.pdf
[12] Note two letters dated June 21, 2007 to the secretary available at http://ncvhs.hhs.gov/070621lt2.pdf and http://ncvhs.hhs.gov/070621lt1.pdf
[13] Note a letter dated February 20, 2008 to the secretary available at http://ncvhs.hhs.gov/080220lt.pdf

technology as specified by the HITECH Act. The intent was to solicit a framing definition from the industry about realistic components necessary to meaningfully use HIT across a 3-year time-frame for offering incentives to providers through ARRA. The testimony was compiled, assimilated, and disseminated to the Office of the National Coordinator for HIT. [14] NCVHS also sent the ONC a set of observations from the hearing.

PRIVACY

Most recently, NCVHS transmitted recommendations designed to inform the Secretary in preparation of the report required by ARRA regarding privacy and security requirements for personal health records that are not operated by HIPAA covered entities, or in other policy deliberations. Since information is likely to be transmitted over the NHIN to populate PHRs in many cases, these new products and services are an integral part of how health IT is changing the landscape. NCVHS identified the possible confusion for consumers between personal health record products or services that are covered by HIPAA and those that may not be, and recommended that the rules be made very clear to consumers. In particular, NCVHS made a number of recommendations that mirror similar requirements of HIPAA and advised that these be applied to PHRs regardless of whether they are covered by HIPAA.

For example, NCVHS said that Consumers should have the right to consent or to withhold consent to uses and disclosures of their information by a PHR supplier, and that the process of consent should be structured in a manner that enhances consumer understanding. It recommended that consumers have a right to an accounting of uses and disclosures, the ability to amend or delete records, and the right to file complaints regarding privacy and security and an appropriate process of redress. NCVHS further recommended that consumers should be informed that information transfers from HIPAA-covered entities to PHR suppliers not covered by HIPAA will place their health information outside the scope of HIPAA.

Similar to the new requirement in the HITECH Act that consumers have access to electronic versions of their medical records, NCVHS stated in its letter that consumers should have the right to an electronic copy of the information in their PHRs. NCVHS expressed concern that consumers who invest time entering data into a PHR should be able to move it to another supplier without being disadvantaged. Therefore, NCVHS recommended that the Secretary encourage PHR suppliers to develop their products in a manner that facilitates interoperability by incorporating national standards for exchange of information, and that if any PHR certification processes are developed, they should incorporate national standards for exchange of information. Moreover, NCVHS recommended that consumers have access to electronic copies of their PHRs in a format that allows transfer directly to, or reentry in, a different PHR.

[14] Note two letters dated May 18, 2009 for *Reporting of Hearing* and June 1, 2009 for *Observations* to the secretary available at http://ncvhs.hhs.gov/090518rpt.pdf and http://ncvhs.hhs.gov/090428rpt.pdf respectively.

V. Conclusions

The NCVHS reaffirms the importance of the HIPAA administrative simplification provisions and continues its careful technical work on HIPAA. Much of NCVHS' advising has focused on the potential and the limits of health IT with respect to privacy, quality, standards, and population health. The pressing need for stewardship to permit multiple uses of health information is a growing emphasis and is reflected in an NCVHS Primer released in 2009. The major areas of work for NCVHS are information policy issues related to health IT and the NHIN, meaningful use of EHRs, health care quality, data stewardship, population health data, privacy and confidentiality, security and standards. In 2009, NCVHS compiled all its landmark recommendations to the Department on privacy and confidentiality, between 2006 and 2008, and issued them as a single volume, to serve as a reference and resource for the field. NCVHS recommends that this volume become the "Roadmap" for privacy and confidentiality in electronic exchange of patient information.

If one single achievement is associated with NCVHS in recent years, it is probably the selection and recommendation of health IT standards that have now become the foundation for interoperability, care coordination, and the measurement of health care quality and outcomes. The HIPAA administrative simplification provisions had directed NCVHS to study and recommend standards for electronic patient medical record information (PMRI). NCVHS recognized this directive as new and strategic, because all of the other HIPAA standards were intended to support the reimbursement and statistical research processes, while the PMRI standards would need to support the patient care process in a real time clinically specific manner. These sets of standards have been adopted virtually unchanged as the foundation for the demonstration of meaningful use of HIT. NCVHS continues to advocate for a streamlined process for the development, adoption, and implementation of these standards.

Federal Government Web Sites for HIPAA Administrative Simplification. In addition to the NCVHS web site, http://www.ncvhs.hhs.gov/, two other web sites containing HIPAA administrative simplification regulations, frequently asked questions, and other helpful materials are: the HHS Office for Civil Rights, http://www.hhs.gov/ocr/; and, the HHS Centers for Medicare & Medicaid Services, http://www.cms.hhs.gov/hipaaGenInfo.