The National Committee on Vital and Health Statistics
The Public Advisory Body to the Secretary of Health and Human Services

The Tenth Report to Congress

On the Implementation of the Administrative Simplifications Provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996

U.S. DEPARTMENT OF HEALTH
AND HUMAN SERVICES

December 12, 2011

The Honorable John Boehner
Speaker of the House of Representatives
H-232, The Capitol
Washington, D.C. 20510

Dear Mr. Speaker:

I am pleased to transmit the Tenth 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. This year the report is a retrospective summary of HIPAA's implementation and a look forward.

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.

This Tenth Report to Congress on the Administrative Simplification provisions of HIPAA reflects a milestone in recognizing the impact of the transition and evolution of health electronic technology. The report summarizes for Congress and the public the current status of the implementation, the successes as well as the impediments to complete implementation, the consequences of these shortcomings and the necessary next steps.

NCVHS serves a unique role in creating a forum for stakeholders to contribute observations and recommendations to the policy-making process, including HIPAA. As a federal advisory committee, it works in partnership with the private sector, other advisory bodies, and the Department of Health and Human Services (HHS).

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/
Justine M. Carr, M.D.
Chairperson,
National Committee on Vital and Health Statistics
Enclosure

Identical letter to:

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

The Honorable Daniel Inouye
President Pro Tempore
United States Senate
Washington, D.C. 20510

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

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

The Honorable John Kline
Chairman
Committee on Education and the Workforce
U.S. House of Representatives
2181 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Fred Upton
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:

The National Committee on Vital and Health Statistics
The Public Advisory Body to the Secretary of Health and Human Services

The Tenth Report to Congress

On the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996

As Required by the Health Insurance Portability and Accountability Act, Public Law 104-191, Section 263

Submitted to the
Senate Committee on Finance and Committee on Health, Education, Labor and Pensions
House Committee on Ways and Means, Committee on Education and Labor and Committee on Energy and Commerce

December, 2011

This report was written by NCVHS Consultant Writer Margaret Amatayakul, in collaboration with NCVHS members and staff.

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory [42 U.S.C. 242k(k)] public advisory body to the Secretary of Health and Human Services in the area of health data and statistics. In that capacity, the Committee provides advice and assistance to the Department and serves as a forum for interaction with interested private sector groups on a variety of key health data issues. The Committee is composed of 18 individuals from the private sector who have distinguished themselves in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. Sixteen of the members are appointed by the Secretary of HHS for terms of four years each, with about four new members being appointed each year. Two additional members are selected by Congress.

NCVHS Membership (See detailed NCVHS roster in Appendix D.)

Justine M. Carr, M.D., Chair
John J. Burke, M.B.A, MSPharm.
Raj Chanderraj, M.D., F.A.C.C.
Bruce B. Cohen, Ph.D.
Leslie Pickering Francis, J.D., Ph.D.
Larry A. Green, M.D.
Mark C. Hornbrook, Ph.D.
Linda L. Kloss, M.A., RHIA, FAHIMA
Vickie M. Mays, Ph.D., M.S.P.H.
Blackford Middleton, M.D., M.P.H., MSc
Sallie Milam, J.D., CIPP, CIPP/G
Len Nichols, Ph.D.
William J. Scanlon, Ph.D.
W. Ob Soonthornsima
Walter G. Suarez, M.D., M.P.H.
Paul C. Tang, M.D.
James M. Walker, M.D., F.A.C.P.
Judith Warren, Ph.D., R.N.

James Scanlon, Executive Staff Director
Deputy Assistant Secretary, Office of Science and Data Policy
Office of the Assistant Secretary for Planning and Evaluation, DHHS

Marjorie S. Greenberg, M.A., Executive Secretary
Chief, Classifications and Public Health Data Standards Staff, Office of the Director
National Center for Health Statistics, CDC

Table of Contents

National Committee on Vital and Health Statistics
Tenth Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996

Executive Summary

By most measures the United States continues to spend a larger than necessary share of health care dollars on administrative processes because of inefficiencies that have resulted from lack of standardization in common administrative transactions. While the precise amount is difficult to pinpoint, estimates are sizeable given that roughly 10-15 percent of the nation's $2.5 trillion annual spending goes to all administrative costs.

Description of HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was expected to play a major role in reducing administrative costs. HIPAA was created to achieve several goals, including making it possible for people to keep health insurance; protecting the confidentiality, privacy and security of healthcare information and helping the health care industry control administrative costs. A main component of HIPAA is Administrative Simplification, which requires the adoption of standards for electronically receiving, transmitting and maintaining healthcare information and ensuring the privacy and security of individually identifiable health information. The HIPAA electronic data requirements for standardized formats and content were intended to move the health care industry from a manual to an electronic system to improve security, lower costs and the lower the error rates.

Status of Implementation

Over the past decade, the Administrative Simplification provisions of HIPAA have contributed to the transformation and modernization of the health care industry in three important ways: 1) laying the groundwork to move the industry from paper to electronic formats in administrative and clinical systems; 2) moving the industry to a common set of standards, from a multiplicity of standards and formats; and 3) establishing a privacy and security framework to ensure protection of health information. Today there is much greater awareness of the importance of standards and the need to protect the privacy of personal health information and enhanced efforts to do so.

However the completeness of these efforts is not known, as neither the Department nor the health care industry has systematically tracked implementation. Moreover the speed of adoption across industry has been disappointing, though in part understandable given the starting point and the process for adoption and implementation. The lack of full implementation of all HIPAA components by all parties involved now threatens the nation’s progress toward reforming the health care system and providing access to quality health care.

Incomplete Implementation of HIPAA Threatens Reform of the Health System

Seamless, secure exchange of health information is essential to improving the health of all Americans and to reforming the system through which care is delivered. Both the incomplete implementation of data standards contained in HIPAA, and its non-universal applicability to all participants threaten the success of health reform. The achievement of the vision of seamless electronic flow of information in a confidential and secure manner has been slow. Progress in achieving the full benefits of administrative simplification and strong privacy protection has been and will continue to be hampered by the following issues:

- The law failed to mandate adoption by all health care parties, (the law requires adoption by all health plans, all health care clearinghouses, and only health care providers that choose to conduct transactions electronically).
- Strong incentives for adoption by health care providers to conduct transactions electronically (such as Medicare's requirement or state laws) are often absent.
- The absence of measures to document benefits has undermined full scale and more rapid adoption.
- The benefits of standardization were compromised by the levels of optionality and variability permitted in the interpretation of the original industry standards.
- Congress prohibited the Department from using the authority under HIPAA to promulgate a final rule or standard for a unique patient identifier.

Necessary Next Steps

HIPAA's goals remain highly relevant with an ever growing need to converge financial, administrative, and clinical data to promote greater quality and efficiency in the health sector, while ensuring the privacy and security of such data. The achievement of the goals is contingent upon a strong commitment by the Department and other stakeholders to realize genuine administrative simplification and privacy protection involving the integration of data from a multiplicity of sources in ways never envisioned when the law was passed.

To realize the vision of HIPAA and adequately address the pressing health needs of an aging America, it is necessary to move boldly and vigorously to complete the standardization needed to effectively and efficiently deliver quality care. Among the most important steps moving forward, we need to:

- Develop meaningful metrics to measure progress
- Identify appropriate incentives to ensure full adoption
- Ensure adoption and implementation of all standards by all entities
- Accelerate the pace to adopt and implement new standards
- Implement more aggressive enforcement
- Synchronize timelines in the adoption and implementation of standards
- Anticipate and address unintended consequences
- Harmonize the implementation of major initiatives

This Tenth Report to Congress, as required by HIPAA,[1] chronicles key milestones, underlying progress, and ongoing work to fully implement all provisions.

General Observations and Findings

- It is hard to overlook the profound impact and transformative effect that the HIPAA Administrative Simplification provisions have had on health care in this country over the past 15 years. Each of the core components of HIPAA Administrative Simplification (transactions, codes sets, identifiers, privacy, security, and semantic interoperability) has been, in its own right, a major force in transforming how the business of health care is conducted in the U.S.

- Despite significant progress in the journey towards administrative simplification, some important shortcomings persist, with much more work remaining ahead.

- It has taken the Department and the industry longer than expected to set the foundational components of administrative simplification, including all the needed regulations, transition to the first set of standards, and implementation of the privacy and security regulations

- Certain components of the HIPAA law have delayed the journey and limited the industry's ability to achieve its overall goals, including the failure to require comprehensive adoption and use of electronic transactions

Observations and Findings Regarding Administrative Transactions, Code Sets and Identifiers

- Significant progress has been made to take the industry from a myriad of non-standard methods of conducting the business of health care to a basic set of core standards for key administrative transactions

- The impact of HIPAA electronic transaction standards, code sets and identifiers on reducing administrative burdens and lowering the proportion of administrative costs to overall health care costs, while important based on some anecdotal accounts from individual health care organizations, cannot be easily documented, quantified or assessed across the industry.

- There were important limitations in the version adopted for the first round of standard transactions, including most notably the level of optionality offered by the standard. This prompted the creation of "companion guides" by each health plan to further refine the optionality of the standard.

- Adoption by all entities of each of the eight core transactions for which standards have been established (claims, claim payment, coordination of benefits, claim status, eligibility, enrollment, premium payment, referral authorizations) has been less than desirable. By some accounts, only 75% of claim submissions are done electronically; 40% of providers and payers exchange eligibility and claim status via the defined standards; 26% of claim remittances are sent electronically and 10% of claims are paid using electronic fund transfers.

[1] See Appendix A for NCVHS Statutory Reporting Requirements for HIPAA

- Medicare, through the Administrative Simplification Compliance Act of 2001 (ASCA) was able to require providers to use the electronic transactions named in HIPAA. With this, they are able to report to-date upward of 97% of Part B (professional) claims and more than 99% of Part A (institutional) claims submitted electronically using the mandated standards. Annual volumes of eligibility inquiry and response transactions have also risen from just over 7 million transactions in 2005 to over 504 million in 2010.

- The pharmacy industry had been independently implementing national standards for several years, and benefited from having the industry-adopted standard named as the national standard for pharmacy transactions.

- Use of electronic transactions by other health care providers including dentists, allied professionals, laboratories, long-term care, is less well documented, although in many cases, these providers use external vendors (clearinghouses, practice management systems) to perform electronically on their behalf the administrative transactions named in HIPAA.

- Adoption and use of established health identifier standards (employer, provider) have been much more pervasive.

    - Designating the Employer Identification Number as the national standard to identify employers in administrative transactions simplified its adoption and use, because all employers already had this number.

    - Establishing a new National Provider Identifier (NPI) was a much larger effort for the entire industry. Today, the NPI serves as the unique identifier for all providers (individuals and entities) that need to be identified in an administrative transaction. The NPI has also been used in other programs and initiatives, extending its value. Still, the NPI has important limitations, including not being required for ALL health care providers and not being able to provide a reliable and timely cross-mapping between individual providers and the entities in which they practice.

    - The Affordable Care Act mandates that the health plan identifier (HPID), originally required by HIPAA, be adopted by October 1, 2012. The pending definition and requirements for the adoption and use of a National Health Plan Identifier will take us one step farther into standardization, interoperability and simplification.

    - A health identifier for individuals remains the final and most challenging identifier to actualize. The result is great difficulty ensuring accurate linkage of an individual's records, essential to activities such as coordination of care or quality measurement. This is a significant roadblock to successful health information exchange. Due to appropriations legislation consistently disallowing expenditure of federal funds to finalize a standard for such an individual identifier, this potential solution to the problem of linking records cannot be fully evaluated.

- The upcoming implementation of the next version of standards for all electronic transactions (5010 for non-pharmacy transactions and D.0 for pharmacy transactions) is expected to take the industry several steps forward towards reaching true administrative simplification. The most significant improvement is the reduction in the optionality of the standards.

- The transition from ICD-9-CM to ICD-10 code sets, scheduled to take place October 1, 2013, represents one of the most significant challenges the health care industry has faced in recent years. The ICD-9-CM coding system (the clinically modified international code set to describe condition/disease of a patient and, for inpatients, the U.S.-based code set to describe the procedure or service delivered) is embedded in every health care provider and health plan system as the basis for each and every claim adjudication and reimbursement decision, as well as evaluation of service utilization, quality of care and patient safety. Changing to the updated and more granular ICD-10 code sets will contribute to improved health and health care. However, it will require major changes within organizations, including business operations, process workflows, and information system applications.

Observations and Findings Regarding Privacy and Security

- The HIPAA Privacy and Security Rules have had a profound effect on how health information is collected, protected, accessed, used, and disclosed within and among health care organizations in this country. The regulations serve as a national reference point, creating an underlying foundation and setting core minimum requirements for how health information is protected.

- HIPAA has raised collective consciousness concerning privacy and security of health information, as can be attested by the number of privacy and security complaints filed with the Office for Civil Rights. At the same time, no assessment of how this volume of complaints compares to the overall number of instances where privacy may have been compromised has been made.

    - From the effective date of compliance in April, 2003 through September 30, the Office for Civil Rights (OCR) has received over 64,126 HIPAA Privacy complaints and has resolved over 91% (over 58,409) through investigation and enforcement (over 14,527), investigation and finding no violation (7,548), and by closing cases that were not eligible for enforcement (36,334). The top five Privacy Rule complaints have consistently included impermissible uses and disclosures of protected health information, lack of safeguards of protected health information, lack of patient access to their own information, uses or disclosures of more than the minimum necessary information, and complaints to the covered entity.

    - Also as of September 30, 2011, and since the authority to administer and enforce the Security Rule was transferred to OCR on July 27, 2009, OCR has received approximately 471 complaints alleging a violation of the Security Rule. During this period, 236 complaints were closed after investigation and appropriate corrective action; and 235 complaints and 66 compliance reviews remain open. The top five Security Rule complaints were in information access management, access control, awareness and training, incident procedures, and device and media control. While the number of Security complaints may seem small in comparison to Privacy complaints, the second most frequent type of complaint to OCR under Privacy has regarded Safeguards.

    - Since becoming effective on September 23, 2009, and as of December 31, 2010, 252 breaches involving 500 or more individuals, which require notification to the subjects of the records, were reported, impacting over 7.8 million individuals. The most common causes were theft; loss of electronic media or paper records containing protected health information; unauthorized access to use or disclose protected health information; human

error; and improper disposal. Over the same period, approximately 30,521 reports of breaches involving fewer than 500 individuals were reported, impacting 62,000 individuals. The majority of small breaches involved misdirected communications about a single individual.

- One of the most important issues with the regulations (traceable back to the HIPAA statute) is the fact that they only apply to 'covered entities' (all health plans, all health care clearinghouses and health care providers who choose to conduct transactions electronically) and their business associates, and not to every entity that has access to or maintains health information about patients and consumers.

- The Congress and the Department of HHS have made important changes over the past five years to improve, enhance, clarify and expand the applicability and enforcement of these regulations, including the adoption of breach notification regulations prompted by the 2009 Health Information Technology for Clinical and Economic Health (HITECH) Act

Observations and Findings on Semantic Interoperability

- HIPAA originally called for uniform data standards for and the electronic exchange of "patient medical record information." Semantic interoperability refers to the communication of structured, codified computational electronic information between organizations in a consistent and unambiguous manner. Uniform data standards ensure that when data are exchanged they hold common meaning, thus enabling semantic interoperability.

- The analysis of terminologies and recommendations made by NCVHS during 2000-2006 laid the groundwork for the adoption of national standard terminologies and vocabularies to codify and document medical information electronically and the inclusion of such standard terminologies in the HITECH "Meaningful Use of Electronic Health Record Technology Incentive Program."

- As the nation continues its journey to enhanced deployment, adoption and use of EHRs, the achievement of full cross-organization semantic interoperability will continue to be one of the most critical goals and milestones in the journey towards administrative simplification and effective and efficient health information exchanges

Other Related Areas

- A number of other legislative initiatives have leveraged HIPAA and its goal for using health information technology to improve the quality and cost of health care and thereby improve health. The Medicare Modernization Act (MMA) promotes the exchange of prescription information. The Drug Enforcement Administration recently adopted standards for electronic exchange of prescriptions for controlled substances. HITECH contributes to further adoption of technical (i.e., message exchange), as well as semantic, interoperability. The Affordable Care Act (ACA) enables greater standardization for the implementation of financial and administrative transactions through operating rules and completed adoption of the HIPAA transaction standards.

The Journey Forward

While there have been important achievements over the past 15 years towards administrative simplification and privacy and security of health information, much work remains. As such, the nation needs to set its course to:

- ***Reinforce the vision*** of HIPAA's Administrative Simplification provisions and stay the course.
- ***Re-state the purpose*** of the overall journey towards administrative simplification with documented evidence of the business case for full adoption and implementation of all required standards.
- ***Reaffirm the need*** for full, across the board adoption and implementation of all transactions by all covered entities.
- ***Map out an integrated framework and approach*** to administrative simplification, electronic health records adoption, health information exchange implementation, health care quality improvement, and health reform.
- ***Extend and improve*** protections of the privacy and security of health information while facilitating appropriate data uses and exchange.
- ***Reassess the value*** by measuring, documenting and sharing results with the public.

The industry will need to continue to 1) refine and adopt improved standards for existing transactions by looking at the next version of these standards and when to implement them; 2) migrate code sets to more refined and mature ones; 3) implement the new operating rules being mandated under ACA; 4) implement new transactions and code sets using defined national standards, including acknowledgment transactions, claim attachments, first report of injury, and others. Additionally, the industry will need to pursue new areas of standardization, such as provider credentialing and enrollment, claim edits, and the applicability of standards to workers' compensation and property/casualty insurance.

The industry will also need to continue to refine, expand and harmonize the implementation of privacy and security requirements in a number of areas, including implementing a national health information privacy and security framework, preserving an applicable degree of state variation without losing semantic interoperability, protecting personal health records, adoption and use of e-consent standards, ensuring data stewardship over secondary uses of data, and defining the applicability of privacy and security policies and regulations to new forms of care delivery included in health reform (i.e., accountable care organizations and health insurance exchanges).

The industry will also continue to see a trend towards convergence of the administrative and clinical message exchange, as the current national and regional health information technology and health information exchange initiatives continue to evolve.

As the creators of HIPAA envisioned, the efficiency and effectiveness of health and health care in the U.S. are improved through modern information technology use. Information technology also presents new challenges for privacy and security that require continued attention. This is the time for all stakeholders to ensure that the journey initiated with HIPAA goes forward with prudent but deliberate actions that rapidly and effectively achieve administrative simplification through compliance with health

data standards. Ultimately, results are measured not only by implementation milestones, but also by realized tangible improvements throughout the health care delivery system.

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 includes Administrative Simplification provisions that require adoption of standards for financial and administrative transactions and code sets. HIPAA also requires protection of the privacy, confidentiality, and security of patient medical record information. This section of HIPAA states that these standards will promote the "efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." While much has been accomplished, much work remains.

This Tenth Report to Congress on the Administrative Simplification provisions of HIPAA is a milestone report for the National Committee on Vital and Health Statistics (NCVHS). It summarizes for Congress and the public:

1. The Journey Taken: What regulations and guidance documents have been promulgated under HIPAA and related legislative initiatives for administrative simplification?
2. Where Are We Now: What has been the impact of the HIPAA Administrative Simplification (herein after referenced simply as "HIPAA") regulations?
3. The Journey Forward: What needs to happen next?

This report also marks the start of transitioning from the original HIPAA regulations to a significant level of activity on administrative simplification through provisions in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Affordable Care Act (ACA) of 2010. Enhancements from both new HIPAA regulations and ACA provisions include:

- Transition to the next versions for current administrative transactions and code sets[2]
- Transition from ICD-9-CM to ICD-10-CM/PCS[3]
- Adoption of standards and implementation specifications for new administrative transactions
- Adoption of standard operating rules for all transactions
- Adoption of a unique health plan identifier
- Implementation of breach notification for protected and personal health information
- Modifications to the Privacy Rule
- Security risk analysis required in the "meaningful use" incentive criteria
- Stepped up enforcement action

[2] Code set is defined by CMS in HIPAA Information Series, 4, Overview of Electronic Transactions and Code Sets, May 2003 as a group of representations for data elements or pieces of information. **Medical code sets** are those used in transactions to identify what procedures, services, and diagnoses pertain to a patient encounter. They currently include ICD-9-CM Volumes 1 and 2, ICD-9-CM Volume 3, National Drug Codes (NDC), Current Dental Terminology (CDT), Current Procedural Terminology (CPT), and Healthcare Common Procedural Coding System (HCPCS). **Non-medical code sets** characterize a general administrative situation. They may include widely used codes such as state abbreviations, zip codes, and race and ethnicity codes; as well as codes specific to the nature of the transactions, such as provider taxonomy codes and claim adjustment reason codes.

[3] Herein the International Classification of Diseases, Tenth Edition, Clinical Modification and its Procedure Code System are abbreviated ICD-10-CM/PCS.

Because the Nation's health care sector is at a critical juncture, this report is designed not only to address the statutory requirements for reporting on HIPAA implementation[4] but also to reflect on the journey taken as a guide to future steps.

In preparing this Report, NCVHS considered the "decade of HIPAA," together with its own six decades celebrated last year.[5] The Committee was created in 1949 to focus on building national and international health statistics. Increasingly it has been called upon to address data standardization and associated data protections as "a signal activity." NCVHS serves a unique role in creating a forum for stakeholders to contribute observations and recommendations to the policy-making process. As a federal advisory committee, it works in partnership with the private sector, other advisory bodies, and the Department of Health and Human Services (HHS).

[4] P.L. 104-191 Health Insurance Portability and Accountability Act of 1996, Section 263 Changes in Membership and Duties of National Committee on Vital and Health Statistics, Subsection 7 Annual Report to Congress on Implementation of Title XI Part C Social Security Act, See Appendix A.
[5] NCVHS: Sixty Years of Making a Difference, June 2010

Section 1: The Journey

1.1 What is HIPAA Administrative Simplification?

The original HIPAA legislation, signed into law in 1996, was a major health reform initiative that consisted of five titles addressing: insurance portability; fraud and abuse, administrative simplification, and medical liability reform; medical savings and tax deductions; group health plan provisions; and revenue offset provisions. Within the Administrative Simplification provisions, NCVHS was given new responsibilities (Appendix A), later expanded under HITECH and ACA, to advise the Secretary on the adoption and implementation of standards. These include:

- Financial and administrative transactions and code sets (adopted in 2000 with compliance required in 2003) and operating rules to enhance standardization of their use (legislated in 2010 with implementations scheduled through 2016).
- Unique health identifiers for employers (2002), providers (2005), health plans (to be implemented by October 2012), and individuals (not yet addressed)
- Standards for health information privacy (effective 2003) and security (effective 2005)
- Data standards for patient medical record information (now referenced more generally as semantic interoperability which applies to all forms of health information technology (HIT), electronic health records (EHR), and health information exchange (HIE), adopted under HITECH regulations issued in 2010.

The Administrative Simplification section of HIPAA contained important defining elements that shaped the evolution of adoption and implementation of standards in the health care industry. In defining 'covered entities' (entities subject to comply with the law) HIPAA stipulated that while payers and clearinghouses were required to implement the electronic transaction standards, implementation of electronic transactions and use of the mandated standards by providers was not required, unless they chose to conduct transactions electronically. To encourage providers to adopt the transactions, the Administrative Simplification Compliance Act (ASCA) of 2001 was enacted, requiring health care claims to be sent electronically to Medicare as of October 16, 2003 with certain exceptions to be granted by the Secretary of Health and Human Services (i.e., very small provider organizations).

Employers, which conduct electronic transactions to enroll employees in health plans, also were not required to use the standard electronic transaction. Additionally, HIPAA exempted important segments of the health care marketplace, particularly workers' compensation and the health component of automobile insurance.

This section of the report summarizes progress that has been made in issuing regulations in support of HIPAA as well as additional, complementary legislation and regulation, in general chronological order.

1.2 What regulations have been promulgated under HIPAA and other legislative initiatives?

1.2.1 Financial and Administrative Transactions and Code Sets

Financial and administrative transactions and code sets, as enumerated and illustrated in Appendix B, were the second set of HIPAA Administrative Simplification provisions to be implemented, soon after

compliance with the HIPAA Privacy regulations took place. As of the writing of this Report, most of the original provisions related to transactions and code sets have been implemented--a long and winding journey with a few places not yet visited. The journey now continues with a new set of administrative simplification provisions included in the ACA legislation. Table 1 provides a summary of the timelines for which the HIPAA and ACA provisions relating to the transactions and code sets have been or are anticipated to be adopted.

Table 1. HIPAA/ACA Transactions and Code Sets Major Milestones

HIPAA/ACA Transactions and Code Sets Major Milestones	**Publication**	**Compliance Required**
HIPAA enacted	1996	
Transactions and code sets, except first report of injury and claims attachments, including ICD-9-CM; ASC X12[6] version 4010, NCPDP[7] Telecom 5.1 and Batch 1.0	2000	2002
Administrative Simplification Compliance Act (ASCA) (provides a 1-year extension for compliance with transactions and code sets and requiring electronic claims for Medicare)	2001	2003
Adoption of transactions and code sets, ASC X12 version 5010, NCPDP D.0 and 3.0 Medicaid Subrogation	2009	2012
Adoption of ICD-10-CM/PCS	2009	2013
Affordable Care Act (ACA) Administrative Simplification provisions for standard operating rules for transactions and code sets	2011	2013-2016
Adoption of health care electronic funds transfer standard and operating rules required under ACA	2012	2014
Adoption of claims attachment standard and operating rules required under ACA	2014	2016
Biennial review of amendments to the transaction standards and code sets and operating rules required under ACA		2014
Health plan certification of compliance required under ACA	2012	2013-2015

While it took more time than expected to finalize and publish the first round of regulations defining standards and code sets for electronic administrative transactions, it is important to consider the significance of this first step. By most measures, this was a major transformative effort that took the entire health care industry from a myriad of non-standard ways of conducting the business of health care to a common set of electronic administrative transaction standards.

[6] The Accredited Standards Committee (ASC) X12, chartered by the American National Standards Institute (ANSI) more than 30 years ago, develops and maintains electronic data interchange (EDI) and XML schemas for the health care, insurance, transportation, finance, government, supply chain, and other industries.

[7] The National Council for Prescription Drug Programs (NCPDP) is a not-for-profit, ANSI-accredited standards development organization developing standards and guidance for promoting information exchanges related to medications, supplies, and other pharmacy-related services.

The first round of standards and implementation specifications selected and adopted for use were the most mature in existence at the time. They had been developed by national and international standard development organizations and data content committees, been tested and were at various levels of use. As a first round of standards, and with several other administrative simplification elements pending (for example, a national provider identifier, and a national health plan identifier), they had to offer a level of optionality to accommodate various state insurance laws, differences in telecommunications capabilities, data formatting issues, and differing data content needs of health plans. The result has been the creation of "companion guides," documents created by health plans to expand, clarify and further refine the requirements in the standards and their implementation guides. As a result, providers were required to adhere to different business requirements for each of the different health plans to which they submit claims and exchange other transactions. The preamble to the Transactions and Code Sets Final Rule noted that before HIPAA there were 400 different formats of the transactions in use. In testimony to NCVHS after the initial implementation of the regulations, it was noted that after HIPAA, more than 1,000 companion guides were developed to clarify formatting and content of the newly mandated standards and implementation specifications.[8]

As explained later in this report, the transition to the next version of the standards and implementation specifications for these transactions will significantly eliminate the optionality of the current version of the standards, and reduce or in many cases eliminate the need for "companion guides." In addition, ACA seeks to further address the gaps and optionality issues associated with the implementation of HIPAA transactions and code sets by calling for the adoption of standard "operating rules for electronic exchange of information not defined by a standard or its implementation specification." ACA also includes requirements for implementation of a healthcare electronic funds transfer (EFT) standard and the claims attachment standard originally included in HIPAA.

1.2.2 Unique Health Identifiers

HIPAA called for four unique health identifiers. Table 2 provides a summary of their adoption.

Table 2. HIPAA Identifiers Major Milestones

HIPAA Identifier Major Milestones	Publication	Compliance Required
HIPAA enacted	1996	
Employer Identifier	2002	2002
National Provider Identifier (NPI)	2004	2007
Health Plan Identifier (HPID)	2011 (expected)	2012
Unique health identifier for individuals	N/A	N/A

The first identifier adopted was the Employer Identification Number (EIN) issued by the Internal Revenue Service. This identifier is used in several administrative transactions to identify the employer of the individual subject of the transaction.

[8] Zubeldia, Kepa. (Ingenix) "From HIPAA to Interoperability," HIPAA Transactions Convergence Project, presentation to NCVHS, April 6, 2005.

The national provider identifier (NPI) became available on May 23, 2005, and was required for use on May 23, 2007. This is a 10-position all numeric, intelligence-free numeric identifier that must be used in all HIPAA-regulated administrative transactions in lieu of all other proprietary, legacy provider identifiers (i.e. identifiers assigned to providers by health plans). Covered providers (individuals, entities) apply for their NPI through the National Plan and Provider Enumerator System (NPPES) and share their NPI with other providers, health plans, clearinghouses, and any entity that may need it for billing purposes. To date over 2.5 million identifiers for individual providers and provider organizations have been issued and are in use. The NPI is also commonly used in other, non-administrative related transactions, systems, programs and initiatives.

ACA mandates that the health plan identifier (HPID), originally required by HIPAA, be adopted by October 1, 2012. Issuance of a HPID requires clarification of the definition of a health plan, types of entities eligible for enumeration with an HPID, and the granularity of the enumeration (i.e., products or lines of business within a health plan, such as Medicare, Medicaid, Commercial, Self-Insured). NCVHS made recommendations to the Secretary to adopt an HPID that follows the ISO Standard 7812, to maintain a directory database to support the enumeration process, to enable the retail pharmacy industry to continue to also use the RxBIN/PCN as an identifier, and to consider the timing of implementing the HPID to ensure adequate time for testing. Regulations are expected sometime in late 2011 or early 2012.

The fourth identifier mandated by HIPAA was a unique health identifier for individuals. Due to public concerns over privacy, in 1999 Congress prohibited HHS from expending appropriations to finalize a standard for such an identifier. This prohibition has been carried over in every appropriations bill since 1999, providing that the prohibition shall hold until legislation is enacted specifically approving such a final standard.[9]

1.2.3 Privacy and Security

The final HIPAA Privacy Rule became effective on April 14, 2003. The HIPAA Security Rule was published in 2003 and became effective on April 20, 2005.

From that time to the present, covered entities and the larger health industry have been facing the challenge of understanding how the regulations apply to them, assessing the methods and likelihood of enforcement, and planning how to implement their new obligations. At the same time, consumers were being exposed to the Privacy Rule, in particular, when they went to their doctors and were presented with “Notices of Privacy Practice” now required by the Privacy Rule.

During the first years, the Office for Civil Rights issued guidance on a variety of topics to assist covered entities with compliance and help consumers to understand and exercise their new rights. OCR issued guidance document with these two major audiences in mind, on topics of interest to both audiences, and in language appropriate to the likely reader. OCR produced an easy-to-navigate website where it is easy to read about the Privacy Rule and to gain access to the specific guidance documents. When

[9] The language of the law states, “[n]one of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual’s capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard. Consolidated Appropriations Act of 2010, Pub. Law No: 111-117, § 511.

responsibility for the Security Rule moved from CMS to OCR in 2009, security guidance was consolidated with the privacy guidance in one place on the OCR website.

For example, for covered entities, OCR has published:

- a question-and-answer decision tool to help determine if an entity is covered by HIPAA
- summaries of the Privacy and Security Rules
- guidance on significant aspects of the Privacy Rule
- guidance on specific security topics, such as the risks of peer-to-peer file sharing applications or digital copiers;
- a sample business associate agreement
- "Fast Facts" with answers to many common questions and misconceptions about patient consent, incidental disclosures, child abuse reporting, electronic media, and other disclosures.
- A special series of documents for small businesses that are covered entities

In November 2008, partly in response to recommendations made by NCVHS in June 2007 regarding the difficulties of health units in schools managing their records, HHS published *Guidance on the Application of FERPA and HIPAA to Student Health Records.*

On the consumer side, OCR has been equally active, issuing guidance explaining the basics of HIPAA rights and the obligations of covered entities in plain language intended for consumers, including consumer brochures in seven languages other than English. OCR also publishes on specific topics from time to time, and has covered:

- Individual's access to their own medical records
- employers and health information
- personal representatives
- access by family members and friends
- court orders and subpoenas.

OCR has also implemented complaint processing, consumer assistance, and investigative functions throughout its regional offices and at HHS headquarters in Washington, DC, and provides easy-to-use forms for submitting a complaint on its website.

On the April 2003 compliance date of the Privacy Rule, HHS had promulgated an interim final rule so as to have enforcement authority in place immediately. Two years later HHS published a proposed rule to collect comments from the public. After consideration of those comments, HHS produced a final enforcement rule in 2006. These rules remain in place, as modified by subsequent developments including the HITECH Act.

In May 2008, Congress completed long contemplated measures to eliminate or reduce as much as possible the potential harmful discriminatory effects of genetic information disclosure. The Genetic Information Nondiscrimination Act (GINA) was enacted to prohibit discrimination in health coverage and employment based on disclosure of genetic information. GINA is divided into two sections, or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment. Title I required modification to the HIPAA Privacy Rule.

OCR promulgated a proposed rule on October 1, 2009, that would modify the Privacy Rule to clarify that genetic information is health information and to prohibit the use and disclosure of genetic information by covered health plans for underwriting purposes, which include eligibility determinations, premium computations, applications of any pre-existing condition exclusions, and any other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. The rule has not yet been finalized.

In 2007, NCVHS heard testimony from 75 organizations from the U.S. and abroad to compile a report, *Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data.* This report included recommendations to:

- Strengthen privacy protections by business associates including clarifying that companies providing data transmission services were business associates.
- Provide guidance on security safeguards and controls
- Provide guidance on de-identification and minimum necessary uses and disclosures of protected health information (PHI)—in general, and as used in quality measurement, reporting, and improvement and research. It has been observed that the lines between use of data for quality and for research are blurred.

Modifications to the Privacy Regulations. In 2010, the first major update to the HIPAA Privacy Regulations was issued, in response to provisions in the HITECH act. These provisions and subsequent modifications to the Privacy Rule included the extension of requirements to business associates, new controls and restrictions on the use of health information for marketing, role of state jurisdictions to act upon HIPAA privacy violations, and new enforcement activities. These are critical issues, as they largely address four of the top five issues in complaints filed with OCR – impermissible uses and disclosures, failure to provide access, disclosure of more than the minimum necessary information, and failure to provide an adequate notice of privacy practices. The proposed rule would also extend the applicability of certain of the Privacy and Security Rules' requirements to the business associates of covered entities, establish new limitations on the use and disclosure of PHI for marketing and fundraising purposes, and prohibit the sale of PHI without patient authorization. The proposed rule would strengthen and expand OCR's ability to enforce the HIPAA Privacy and Security provisions. In addition to these topics, the preamble to the proposed rule observed that HITECH called for study of several other privacy issues which would be addressed in subsequent regulation, including minimum necessary, de-identification, definition of "psychotherapy notes," and authorization for use of PHI in future research.

Breach Notification. The HITECH Act required the Secretary to issue breach notification requirements for HIPAA covered entities and their business associates. OCR issued a Breach Notification Rule as an interim final regulation in 2009, effective for breaches discovered on or after September 23, 2009. The Rule requires covered entities to notify individuals, the Secretary, and in some cases, the media, of breaches of unsecured protected health information. In the case of a breach at a business associate of a covered entity, the Rule requires the business associate to inform the covered entity of the breach so that the proper notifications can be made. From September 2009 to the end of September 2011, OCR reported receiving 360 reports of breaches involving more than 500 individuals. In total, these breaches affected 16 million individuals.

These larger breaches commonly involve theft or loss of computers or electronic media housing unencrypted health information. For example, the three most extensive breaches, involving the health

information a total of almost 9 million individuals, were due to the loss of unencrypted backup media or disk drives. The next two largest breaches, which affected over 900,000 individuals, resulted from the theft of desktop computers. Finally, one breach involving the health information of over 175,000 individuals resulted from a system error that misprinted several thousand documents.

Additionally, OCR has received over 36,000 reports of breaches involving fewer than 500 individuals. The majority of these reports involve misdirected communications and affected just one individual each. Often, the clinical or claims record or other health information of one individual is mistakenly mailed or faxed to another individual.

Accounting of Disclosures. HIPAA required that covered entities maintain an accounting of certain disclosures and provide information of such disclosures to consumers upon request. HITECH expanded the types of disclosures for which an accounting was required to include disclosures done for treatment, payment and operations through an electronic health record. In 2011 HHS published proposed regulations to address this new requirement.

The HITECH Act also significantly strengthened the Department's ability to enforce against entities for violations of the HIPAA Rules by revising and greatly increasing the civil money penalty amounts that may be imposed for violations. Prior to the HITECH Act, the Department had authority to impose a civil money penalty against a covered entity of up to only $100 for each violation, with a calendar year limit of $25,000 for all identical violations. The HITECH Act greatly enhanced the penalty scheme by creating four categories of violations that reflect increasing levels of culpability – from circumstances where the entity did not know of the violation to circumstances of willful neglect, and by attaching to each tier amounts that significantly increase the minimum penalty amount for each violation. Now, covered entities are subject to penalties that range from $100 to $50,000 or more per violation, with a calendar year limit of $1.5 million for identical violations. OCR testified before the Congress in November 2011 that the increased penalty amounts available to the Department reinvigorated covered entities' attention to compliance. The Department is able to use these amounts not only for purposes of pursuing civil money penalties but also in terms of determining and negotiating settlement payments with covered entities that have agreed to resolve issues of noncompliance by entering into resolution agreements with the Department.

A resolution agreement is a contract between the Department and a covered entity to settle potential violations and is accompanied by a corrective action plan in which the covered entity agrees to perform certain obligations, such retraining staff, and to make reports to the Department, generally for a period of three years. These agreements are reserved to settle investigations with more serious issues and outcomes and generally include payment of a settlement amount. When a case cannot be resolved informally through corrective action, HHS seeks to impose a civil money penalty.

In sum, several legislative and regulatory actions have been taken to address many privacy and security concerns. Table 3 lists major privacy and security initiatives since the Privacy and Security Rules were published.

On a parallel track, since the Privacy and Security Rules became effective, policy makers, privacy advocates and the health care industry in general have been engaged in defining new ways to enhance privacy and security, especially as further adoption of health information technology, health information exchange, and nationwide health information exchange have come to the forefront.

Table 3. Privacy and Security Initiatives Since HIPAA

Privacy and Security Initiatives Since HIPAA	Publication	Compliance Required
HIPAA Privacy Regulations	2000	2003
HIPAA Security Regulations	2003	2005
Delegation of authority for the Security Rule to the Office for Civil Rights and investigative staff in regional offices to expand compliance reviews and onsite investigatory methods	2009	2009
Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to unauthorized Individuals for Purposes of the Breach Notification Requirements under HITECH	2009	2009
Interim Final Rule on Breach Notification	2009	2009
Interim Final Rule on Enforcement increased the size of the civil monetary penalties, clarified that a person can be in violation of HITECH and HIPAA, requires civil penalty for noncompliance due to willful neglect; also authorizes State Attorneys General to take enforcement action against HIPAA violators.	2009	2009
Request for information and subsequent notice of proposed rulemaking on extending the accounting for disclosure requirements to disclosures for treatment, payment, and operations from electronic health records.	2010-2011	
Notice of proposed rulemaking on several modifications to the HIPAA Privacy Rule required by HITECH, including expansion of the rules to business associates.	2010	
Advance notice of proposed rulemaking to enhance protections for research subjects and reduce burden, delay, and ambiguity for investigators, including consideration for the adoption of the HIPAA Privacy and Security Rules in lieu of the Common Rule for determining what constitutes “individually identifiable,” a “limited data set,” and “de-identified information	2011	

1.2.4 Semantic Interoperability and Other Health Information Technology

Semantic interoperability is the ability to exchange data with common meaning, typically via adoption of standard terminologies.

Originally, HIPAA called for NCVHS to make recommendations for uniform data standards for the electronic exchange of “patient medical record information.” An extensive analysis of terminologies was made between 2003 and 2006, significantly contributing to the federal Consolidated Health Informatics (CHI) initiative.

The analysis of terminologies and recommendations laid the groundwork for inclusion of terminology standards in the CMS Meaningful Use of Electronic Health Record Technology Incentive Program. In

2009 the HIT Standards Committee recommended the adoption of SNOMED CT (or ICD-9-CM) for documenting the problem list in electronic health records, LOINC for lab results, and RxNorm for medication documentation. These recommendations were adopted in regulations later on as part of the Meaningful Use program and the certification program for EHR technology.

Also contributing to semantic interoperability through standard data sets, are the ASTM International Continuity of Care Record (CCR) standard and the HL7 Continuity of Care Document (CCD) standard. These call for standardization of health information content for provision of health summaries. They have also been adopted as standards under the Meaningful Use program and required for use in certified EHR technology, and have become adopted by some vendors of personal health records.

HL7 standards for structuring and exchange of data among provider entities and with public health have also been included in the certification criteria for EHR technology in the meaningful use incentive program.

1.2.5 Other Legislation

Other legislation also has addressed the need for data standards. The Medicare Modernization Act of 2003 directed adoption of standards for electronic prescribing transactions and code sets. Subsequently, the Drug Enforcement Administration (DEA) and Department of Justice (DOJ) worked with CMS and HHS to address utilizing electronic prescribing for controlled substances. The DEA published an interim final rule on e-prescribing in 2010.

1.2.6 NCVHS Contributions to Administrative Simplification

As suggested by the discussion above, HIPAA's Administrative Simplification provisions have resulted in considerable progress toward standards adoption. In its advisory role to HHS and the Congress, NCVHS has been in a unique position to hold public hearings, learn about what works and what does not work, and take the pulse of the nation with respect to administrative simplification. As a result, over the past 15 years, NCVHS has been able to frame and construct recommendations that have had considerable impact on the success of administrative simplification, as well as to continue to press for further initiatives. Since HIPAA was enacted, NCVHS has written 73 letters to the Secretary concerning HIPAA-related matters. Table 4 provides the breakdown of such letters.

Table 4. NCVHS Letters to the Secretary Concerning HIPAA-Related Matters

HIPAA-Related Topic	Number of Letters
Transactions and Code Sets required by HIPAA (TCS)	14
Operating Rules (OR)	3
Identifiers (ID)	4
Privacy and Security	21
Patient Medical Record Information (PMRI)	9
Nationwide Health Information Network	6
e-Prescribing (e-Rx)	7
"Meaningful use" (MU)	3
Personal Health Records (PHR)	3
Data stewardship	3
Total letters	73

More important than the number of letters, however, is the broad range of topics within the "HIPAA journey" and the extent to which there is congruence of topics across all NCVHS data standardsand protection interests and with other legislation in addition to HIPAA. For example, the ability to appropriately represent mortality and morbidity data across systems is a cross-cutting concern of the Subcommittees on Standards, Quality, and Population Health, and certainly is a key element of PHI that requires privacy protections. Appendix C identifies HIPAA topics and associated standards in which NCVHS has played a role and summarizes how NCVHS subcommittees demonstrate their internal congruence and the relationship of the Committee's HIPAA work with respect to various other legislative initiatives.

Section 2: Where Are We Now?

In any journey, it is always useful to take stock of the distance traveled and what remains. Section 1: The Journey focuses on *setting the foundation for getting the journey started*, including all the initial regulatory process and the start of implementation of standards;. Section 2: Where Are We Now focuses on *adoption and implementation*, including the extent to which regulations have been implemented and embraced, and their impact to date.

In its first HIPAA report covering 1997, NCVHS observed that administrative overhead in the health care delivery system is huge and the burden of these costs affects everyone in the system – from the consumer to the provider, hospital, health plan and employer, with the consumer ultimately shouldering the majority of the burden and directly experiencing its negative effects. It further observed that up to $9 billion per year could be saved by reducing administrative overhead – which would enable freed up resources to be spent on improving the quality of the clinical aspects of health care. Obviously, HIIPAA held great promise for administrative simplification.

While HIPAA administrative simplification has had a transformative effect in the way the business of health care is conducted in the U.S., the full extent of adoption and the effect it has had on simplifying health care administration is difficult to quantify and ascertain. HIPAA did not require analysis of the effects of its provisions, hence evidence that progress has been made is largely anecdotal. Certainly a "second phase" of administrative simplification being initiated through recent HITECH and ACA legislation suggests further improvement is needed and signals the intent for continuous improvement.

2.1 What Has Been the Effect of HIPAA Transactions and Code Sets and Identifiers?

2.1.1 Adoption of Version 4010 Transactions and Code Sets

To consider the impact of the transactions and code sets component of HIPAA, several reports and letters enable some important comparisons and critical observations.

With respect to percent of health care expenditures devoted to administration, very limited generalizable evidence is available to define the degree to which implementation of standards for electronic administrative transactions and code sets in health care have had a significant effect in reducing administrative costs. Thus far, evidence points to some gains in the reduction of administrative costs, but these costs remain significantly higher costs as a proportion of total health care costs in the U.S. than in most other industrialized countries. For Example:

- The Office of Technology Assessment, United States Congress, *International Comparisons of Administrative Costs in Health Care* in September 1994 estimated that in the U.S., private insurers were incurring 7.2 percent of their expenditures on administration, broken out as 14.1 percent for private insurers and 5.2 percent for public programs.

- The Commonwealth Fund[10] in July 2009, estimated that national health care expenditures devoted to insurance administration were at about 7.5 percent of total health care expenditures; and compared the U.S. with France at 6.9 percent– the next highest reporting country, and with Finland at 1.9 percent – the lowest reporting country.

Several important considerations have affected the rate of adoption of the various transactions among covered entities.

- A National Progress Report on Healthcare Efficiency is periodically produced by Emdeon Business Services.[11] Its 2010 report estimates that in the *private sector*, only 75 percent of claims submissions are done electronically, 40 percent of providers and payers exchange eligibility and claim status information via the standard transactions, 26 percent of claims remittances are sent using the standard transaction, and 10 percent pay claims electronically through electronic funds transfer (EFT).

- Medicare mandates electronic claims via the Administrative Simplification Compliance Act of 2003. Its data reveal that in 2000, 82.28% of Part B (professional) claims and 97.55% of Part A (institutional) claims were submitted electronically, using the HIPAA-mandated standard (ASC X12 837 standard; rising in 2010 to 97.55% of Part B claims and 99.86% of Part A claims. Annual volume of eligibility inquiries and responses (ASC X12 270/271) has also risen significantly, from slightly more than 7 million transactions in 2005 to over 504 million in 2010.

This difference illustrates the effect of the original provision of the HIPAA statute that allows providers to *choose to conduct transactions electronically*, and only when they choose to do so electronically, be required to use the standards defined in regulations.

Another important consideration is whether the transactions are used directly among the providers and payers, conducted via clearinghouses, or implemented through direct data entry (DDE) systems (generally, web-based interactive systems that allow providers to conduct transactions one at a time). Although the data cited above do not address this point, the Emdeon report does offer some suggested explanation for the lack of full adoption, such as reluctance by vendors to build the necessary software for non-revenue related HIPAA transactions (such as the eligibility and claims status notification transactions) and reluctance by some payers to robustly implement the HIPAA non-revenue transactions. The process for providers to sign up for using EFT is a manual process not standardized across payers.

One of the most compelling arguments for adopting the standard transactions and code sets is the business case behind them, but full compliance of all parties involved is required. In its 2009 briefing paper on *Understanding the HIPAA Standard Transactions: The HIPAA Transactions and Code Set Rule*, the American Medical Association (AMA) sought to emphasize to its members that HIPAA was not just about privacy and security, as commonly perceived. It encouraged use of the HIPAA standard

[11] Emdeon is health care clearinghouse and supplier to providers and payers of claims and payment management services. It produces the National Progress Report on Healthcare Efficiency. U.S. Healthcare Efficiency Index.

transactions to improve the medical practice claims management cycle as it reminded its members of the upcoming adoption of version 5010 transaction standards. The paper observed, however, that "some health insurers still have not adopted all of the standard transactions or implemented the code set edits and rules." The paper cites costs to providers when a health insurer does not accept electronic claims, create electronic remittance advice, or enable use of the eligibility verification standards (all of which run against the HIPAA requirements for health plans). The paper urges physicians to ask health plans to comply with the standard transactions, and if found not to be in compliance, to file a complaint.[12]

Finally, a measure that may signal impact of a regulation is the volume of complaints. CMS reports that since October 2003, 728 complaints have been filed regarding the Transactions and Code Sets Rule. Of those, 78 have resulted in Corrective Action Plans (CAPs) where an entity deemed partially compliant or non-compliant is allowed to prepare, submit, and implement a plan to take corrective action which is monitored by CMS regularly. No financial penalties have been levied. Whether complaints about transactions and code sets are a valid measure of impact is uncertain, however, as some testifiers to NCVHS over the years have alluded to the fact that many providers fear retaliation for filing formal complaints.

2.1.2 Readiness for Version 5010 Transactions and Code Sets

Clearly the new 5010 version of the transaction standards, to be implemented January 1, 2012, and the adoption and implementation of the ICD-10-CM/PCS code set (October 1, 2013) seek to overcome some of the issues with adopting the original HIPAA transactions and code sets. While the update to 5010 may pose important operational transition challenges, the change to ICD-10-CM/PCS constitutes a very complex, end-to-end changeover. This challenge has significant ramifications, not only on the benefits directly able to be accrued from their implementation but also on being able to adopt other health information technologies such as electronic health records and health information exchange. Consistently it is observed that resources put to any one project draw down the ability to address other projects. NCVHS is closely monitoring implementation progress of all aspects of administrative simplification through periodic hearings, published reports, testimony, CMS testing data, and ONC reports on incentives uptake.

Some key findings with respect to **provider readiness for version 5010** include:

- "Small to medium providers (hospitals with fewer than 400 beds or physician practices of fewer than 50 physicians) are not actively preparing for HIPAA 5010 [revisions to the transactions and code sets]" was identified by Gartner[13] in February 2010.

- Confirming Gartner's findings, the Medical Group Management Association (MGMA)[14] on June 15, 2011 released results of a recent survey it conducted, finding that only 9.2 percent of practices had

[12] Understanding the HIPAA Standard Transactions: The HIPAA Transactions and Code Set Rule, 2009. The AMA Practice Management Center, American Medical Association. page 6.
[13] Gartner, Inc. is an information technology research and advisory company, providing the report, Industry Planning for Implementation of HIPAA Modifications: Version 5010, D.0, 3.0 and the ICD-10-CM/PCS Code Sets to CMS on February 2010 under Engagement: 222895110.
[14] MGMA is a membership association for professional administrators of medical group practices representing physicians providing approximately 40 percent of health care services in the U.S. Its press release "Challenges Persist for Medical Groups Trying to Meet HIPAA Version 5010 Compliance Date" was published June 15, 2011.

done internal testing and 40 percent had yet to schedule internal testing, where guidelines call for testing completion by the end of 2010. In addition, only 29 percent of medical groups reporting believed their current practice management system software would permit them to use version 5010.

- Progress is being made by (larger) hospitals, as evidenced by the fact that 63 percent of respondents to the Healthcare Information Management and Systems Society (HIMSS) [15] Third Semi-Annual Survey of 5010/ICD-10-CM/PCS Readiness in December 2010 had a "5010 project" as compared to only 38 percent of respondents six months earlier. HIMSS findings also showed that about half of providers are focusing their efforts on the second half of 2011, with 30 percent of respondents indicating they did not know when they would start testing.

- Testing progress was also a concern of the Workgroup on Electronic Data Interchange (WEDI).[16] In testimony to NCVHS on June 17, 2011, WEDI reported on its most recent survey that NCVHS Level 1 (internal) testing recommendations have not yet been met and that most Level 2 (external) testing is expected to occur in the last six months of 2011. From a historical perspective, WEDI also found "difficulties in completing testing" to be a significant factor in originally adopting the 4010 version of the standards.[17]

- CMS conducted a National 5010 Testing Day on June 15, 2011, with only 349 Medicare fee-for-service providers participating. Of the trading partners who responded to a follow-up survey conducted by CMS after the testing day, only 32 percent said they were felt ready for the January 2, 2012, implementation date. In follow up, CMS announced that it would dedicate a full week to testing, August 22-26, 2011. Since June 2010, Medicare staff members have been participating in at least two public events per month to work with stakeholders in preparing for version 5010.

Findings with respect to **health plan readiness for version 5010** are mixed:

- The HIMSS survey identifies that two thirds of provider respondents are concerned that their payers would not be ready to pay claims and process other transactions in the 5010 format on time, and about half had doubts about their software vendor's ability to deliver 5010 compliant versions and their clearinghouses to process 4010 and 5010 transactions in time for adequate testing and implementation.

- In the survey conducted by Gartner, however, health plans were viewed as "making good progress and being on track for 5010 compliance" with almost all large health plans "progressing with minimal issues." Gartner reported that health plans view 5010 as "primarily a

[15] HIMSS is a not-for-profit organization focused on providing leadership for the optimal use of information technology and management systems for health care, frequently conducting surveys of interest to its members and others, including the ICD-10-CM/PCS/5010 Industry Readiness Survey: Progress on 5010 but Challenges Ahead. December 2010.

[16] WEDI is a non-profit membership organization of providers, health plans, consumers, vendors, government organizations, and standards groups committee dedicated to the implementation of electronic commerce in health care. WEDI contributed extensive data on the cost/benefit analysis for the compilation of the HIPAA Transactions and Code Sets Rule. Laurie Darst (Mayo Clinic; Co-Chair, WEDI Strategic National Implementation Process [SNIP]) provided WEDI's Statement to HHS NCVHS Subcommittee on Standards, June 17, 2011.

[17] Jones, Ed. (Chair, WEDI) Letter to Secretary of HHS, March 8, 2004

version control exercise with minimal business impact." Gartner's report also suggests that retail pharmacies with respect to D.0 and 3.0 upgrades are slightly ahead of payers in their 5010 upgrades, but– with still 11 months to go – all were facing the final phases of testing and production rollout.

- WEDI observes that with the implementation of 4010, many providers had to undergo a major systems upgrade, but that for 5010 only approximately one-third were undergoing such an upgrade. For health plans, however, a slightly higher number of respondents were doing a major conversion as part of their 5010 implementation, some incorporating ICD-10-CM/PCS components.

A critical finding from all of the surveys is that the 5010 upgrade and ICD-10-CM/PCS project are competing for the same resources within a health care organization (and for providers with the same resources as implementation of EHR for earning meaningful use incentives) and that delays in the 5010 compliance will impact the ability to achieve ICD-10-CM/PCS compliance.

With respect to the ICD-10-CM/PCS implementation:

- Hospital Providers are making important progress on ICD-10-CM/PCS, albeit at a slower pace than for 5010 according to HIMSS. Staffing and funded projects for ICD-10-CM/PCS increased from 30 percent in May 2010 to 47 percent in December 2010. Some 56 percent of respondents had started and 13 percent of respondents had completed their ICD-10-CM/PCS impact assessments. This is consistent with the North Carolina Health Information and Communications Alliance[18]/WEDI Alternative ICD-10-CM/PCS Timeline suggesting providers complete their preliminary impact assessment by January 31, 2011. A different survey from AHIMA, completed in August, 2011, shows a much higher percentage of respondents indicating that they have started work on ICD-10 planning (85% from 62% from the previous year). The HIMSS survey, however, also reports that some 39 percent of respondents plan to use cross walks for their native ICD-10-CM/PCS coding, despite caution from the National Center for Health Statistics (NCHS) that cross walks can never be 100 percent accurate. Finally, the HIMSS survey results also show positive synergy between ICD-10-CM/PCS and EHR implementation, as one third of respondents indicated they would be leveraging efforts to comply with the incentive program for meaningful use of EHR technology.

- WEDI, in testimony to NCVHS on June 17, 2011, expressed concern that all stakeholders – and especially providers – are underestimating the impact of the ICD-10-CM/PCS effort and that testing is lagging behind the NCHICA/WEDI- recommended schedule, including the revised timeline that was adjusted to accommodate organizations that got a late start. It suggested that there be continued education and outreach on business implications of ICD-10-CM/PCS and emphasis that the compliance date will remain October 1, 2012.[19]

[18] NCHICA is a nonprofit consortium of over 240 organizations that lead demonstration projects, host educational events, foster collaborative efforts, and support initiatives to promote the use of standards-based IT in health care. It collaborated with WEDI to develop a schedule for planning adoption of ICD-10-CM/PCS.

[19] Daley, Jim. (Director, IS Risk & Compliance, BCBSSC; Chair-elect, WEDI and Co-chair WEDI ICD-10-CM/PCS work group) Statement to HHS NCVHS Subcommittee on Standards, June 17, 2011.

- For health plans, WEDI is finding that ICD-10-CM/PCS planning is a much bigger project than 5010; more like a Y2K project in scope and criticality. In addition to making the conversion, there must be plans for dual processing and/or crosswalk utilization during the transition. Key business decisions must be made, recognizing the potentially higher cost and level of risk but shorter time to implement associated with the cross walk solution. Some payers' concerns center around specific ICD-10-CM/PCS issues, such as whether payers would receive the codes on schedule, the impact of the implementation process on provider relationships, and the fact that the entire supply chain from provider to clearinghouse to payer and back to provider would be impacted by the timing of the codes.

- Gartner's 2010 survey observes that small providers are very dependent on vendors to provide software and typically do not employ certified coders. As a result, these providers are worried that claims based on ICD-10-CM/PCS will have coding issues, increasing costs of remediation.

2.2 What Have been the Effects of HIPAA Privacy and Security Rules?

This assessment of the impact of the Privacy and Security Rules is largely based on testimony to NCVHS, private sector surveys, and data on complaints filed with OCR.

2.2.1 Privacy Rule

HIPAA Privacy has had a profound effect on how health information is collected, accessed, used and disclosed within and between health care organizations in this country. To date, the regulations serve as a national reference point, underlying foundation, and core minimum requirements for how health information is protected.

Over the years, various commentators have observed the perception that the Privacy and Security Rules lack strong enforcement. Contrary to these perceptions, the number of privacy complaints filed certainly suggests that HIPAA has raised collective consciousness concerning privacy of individually identifiable health information. As of September 30, 2011, and since the compliance date in April 2003, OCR has received over 64,126 HIPAA Privacy complaints and has resolved over 91% (over 58,409) through investigation and enforcement (over 14,527), investigation and finding no violation (7,548), and through closure of cases that were not eligible for enforcement (36,334).

OCR reports that the top five Privacy Rule complaints have consistently included impermissible uses and disclosures of protected health information, lack of safeguards of protected health information, lack of patient access to their protected health information, uses or disclosures of more than the minimum necessary protected health information, and complaints to the covered entity.

It is noted, however, that there have only been six resolution agreements, one in 2008, one in 2009, two in 2010, and two in 2011. The first and only civil monetary penalty was not levied until February 4, 2011. Several recent legislative and regulatory initiatives have provided OCR and HHS the impetus to move forward with such actions. In addition, the incorporation of a security risk analysis as a requirement for qualifying for meaningful use of EHR technology incentives has reinvigorated compliance activities for both the Privacy and Security Rules.[20] In May, 2011, the HHS Office of the Inspector General released a

[20] OCR Enforcement Highlights, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html Accessed 10-24-11.

Nationwide Rollup Review of the CMS HIPAA Oversight, reporting on security audits in 7 hospitals that identified 151 vulnerabilities in the systems and controls intended to protect electronic protected health information, of which 124 were categorized as high impact.

2.2.2 Security Rule

Anecdotal evidence suggests that HIPAA is viewed by many providers to be primarily about privacy.[21] The news media have certainly contributed to this focus, as they regularly report on public concerns about privacy of their health information. However, with respect to the Security Rule, as of September 30, 2011 and since the authority to administer and enforce the Security Rule was transferred to OCR on July 27, 2009, OCR has received approximately 471 complaints alleging a violation of the Security Rule. During this period, 236 complaints were closed after investigation and appropriate corrective action; and 301 complaints and compliance reviews remain open.[22] When CMS was administering the Security Rule, it had reported that the top five security complaints were in information access management, access control, awareness and training, incident procedures, and device and media control. While the number of Security complaints may seem small in comparison to Privacy complaints, it can be observed that the second most numerous complaint to OCR under Privacy has been regarding Safeguards, widely described as the "mini-Security Rule" within the Privacy Rule. The Safeguards standard addresses the requirement for administrative, technical, and physical safeguards to protect against any intentional or unintentional use or disclosure in violation of the standards and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Another indicator of Security Rule impact may be the number of breaches requiring notification. From implementation of the breach notification rule on September 23, 2009 to December 31, 2010, 252 breaches involving 500 or more individuals were reported, impacting over 7.8 million individuals. The most common causes were theft; loss of electronic media or paper records containing protected health information; unauthorized access to, use, or disclosure of protected health information; human error; and improper disposal. Over the same period, approximately 30,521 reports of breaches involving fewer than 500 individuals were reported, impacting 62,000 individuals. The majority of small breaches involved misdirected communications.[23]

The hITECH Act added as requirement for breach notification by vendors of non-HIPAA covered personal health records, to be enforced by the Federal Trade Commission (FTC). Much as with the OCR Breach Notification Rule, the FTC lists on its web site breaches from vendors of personal health record affecting over 500 individuals. Between October 23 and December 15, 2009, Microsoft Corporation posted 13 breaches affecting one individual in each case. The FTC has not posted health breaches for 2010.[24]

Because Security Rule violations are more difficult for the public to recognize, health care stakeholders have relied upon other means to assess the Security Rule state of affairs. Since 2008, HIMSS has

[21] Understanding the HIPAA Standard Transactions: The HIPAA Transactions and Code Set Rule, 2009. The AMA Practice Management Center, American Medical Association. Page 1.
[22] OCR Enforcement Highlights. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html Accessed 10-24-11.
[23] Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2009 and 2010, U.S. Department of Health and Human Services, Office for Civil Rights. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf Accessed 10-24-11.
[24] Breach Notices Received by the FTC. http://www.ftc.gov/privacy/healthbreach/Breach-Notices-Received-by-the-FTC.pdf Accessed 10-24-11.

conducted a security survey to advise its members on the general security environment and commonly used controls. Its *2010 HIMSS Security Survey*[25] was also supported by the Medical Group Management Association (MGMA) to encourage additional representation from medical groups and ambulatory care in general. Spending is often a measure of attention paid to a compliance matter. According to the HIMSS survey, spending on security as a percent of the overall IT budget ranges from less than 1 percent to more than 12 percent, but the majority of organizations spend within the 1 to 3 percent range. Despite the recent breach notification legislation, spending has remained relatively constant throughout the life of the surveys.

The HIMSS survey also found that formal risk analysis is conducted by 76 percent of respondents and nearly all (91 percent) include internal threats in the risk analysis – although this practice varies significantly between hospitals (94 percent) and medical groups (81 percent). Risk analysis appears critical to Security Rule compliance, as 70 percent of respondents reported that a lack of effective security controls that pose a serious or significant risk to patient information was identified during the risk analysis. The Meaningul Use incentives may improve these numbers significantly, as risk analysis is one of the required components of earning the incentives.

While the HIMSS survey is replete with data points, an additional observation it makes with respect to compliance with recent breach notification is that data encryption during transmission was used in only 68 percent of hospitals and mobile device encryption was used in only 45 percent of hospitals. There was significantly lower adoption of encryption (48 percent and 15 percent respectively) in medical groups.

2.3 What Has Been the Effect of HIPAA Semantic Interoperability?

Measuring the effect of terminology standards is more difficult than measuring either adoption of the transactions and code sets standards or privacy and security standards. However, it is clear that such standards are important to facilitate interoperability. Walker, *et al*.[26] estimated that interoperability (including standard terminologies) could yield a net value of $77.8 billion once fully implemented. The Consolidated Health Informatics (CHI) initiative, referenced in section 1.2.4 of this report, contributed significantly to the recommendations made by the HITSP for the Nationwide Health Information Network specifications.

Shafarman[27] describes the use of HL7 v3 Development Framework (HDF) to harmonize data standards between HL7 and NCPDP for e-prescribing. Although more widely used in other parts of the world, HL7 v3 HDF contributes to semantic interoperability between other U.S.-adopted standards as well, such as HL7's Clinical Document Architecture (CDA) and ASTM's Continuity of Care Record (CCR) to form the Continuity of Care Document (CCD) – use of either of which are required in the HITECH meaningful use of EHR technology incentive program. HL7 Clinical Domain Models (DCM) also provide a new way of structuring medical knowledge, data specifications, and terminology.[28] Still, it has been reported by

[25] Healthcare Information Management and Systems Society (HIMSS), 2010 HIMSS Security Survey, November 3, 2010.
[26] Walker, J. et al., 2005 (January 19). The value of health care information exchange and interoperability. *Health Affairs*, Web Exclusive: http://content.healthaffairs.org/content/early/2005/01/19/hlthaff.w5.10.citation
[27] Shafarman, M. 2004 (August 23). HL7 – NCPDP E-Prescribing Harmonization: Using the v3 HDF as a Basis for Semantic Interoperability. Presentation as chair of HL7 and Applications Architect, Oracle Corporation.
[28] van der Zel, M. 2010. Bridging the Gap Between Software Developers and Healthcare Professionals. Hospital Information Technology Europe, 3(2):20-22.

Kuperman, *et al*.[29] that "providing data [in the Nationwide Health Information Network Trial Implementation] in specified terminologies … is a significant challenge, mainly because the participants' source systems used proprietary concept identifiers and translation services were not readily available."

As the nation embarks on enhanced deployment of EHRs with the HITECH incentives for meaningful use of certified EHR technology, which incorporate the recommended standard terminologies, it can be anticipated that early challenges from the Nationwide Health Information Network Trial Implementations will be mitigated over time.

[29] Kuperman, G.J., et al. 2010. Developing data content specifications for the Nationwide Health Information Network Trial Implementations. *Journal of the American Medical Informatics Association*, 17(1):6-12.

Section 3: The Journey Forward

While there have been important achievements over the past 15 years towards administrative simplification and privacy and security protections for health information, much work remains.

Rulemaking, enforcement, or government funding for pilots and trial implementations are not sufficient to achieve full adoption of standards. In testimony at the NCVHS June 2010 hearings on operating rules, testifiers[30] spoke to existence of a clear business case for their *voluntary* adoption of the Council on Affordable Care (CAQH) Committee on Operating Rules for Information Exchange (CORE)[31] operating rules. Health care is grounded in performing actions based on evidence and not hypothesis. Without such clear and compelling evidence, full adoption of any intended action in health care is difficult.

As such, the nation needs to set its course to:

- ***Reinforce the vision*** of HIPAA's Administrative Simplification provisions and stay the course. The path has been laid out through regulation, guidance documents, and stepped-up enforcement. But the journey forward must *ensure results* in the form of true quality and cost improvements.

- ***Re-state the purpose*** of the overall journey towards administrative simplification with documented evidence of the business case for full adoption and implementation of all required standards

- ***Reaffirm the need*** for full, across the board adoption and implementation of all transactions by all covered entities.

- ***Map out an integrated framework and approach*** to administrative simplification, electronic health records adoption, health information exchange implementation, health care quality improvement, and health reform, supported by health information technology. HITECH and ACA call for important enhancements to all aspects of administrative simplification. Much has changed since HIPAA was enacted in 1996 and it can be anticipated that the pace of change will continue to increase.

- ***Extend and improve*** protections of the privacy and security of health information while facilitating appropriate data uses and exchange

- ***Reassess the value*** by measuring, documenting and sharing results with the public. As noted above, the difference between implementation and adoption is very important – but it is also very difficult to measure. However, measurement of impact is critical to achieving results. In 2003, NCVHS made the recommendation for HHS to develop methodologies and collect baseline data for analyzing the effects of the Privacy Rule. It was observed that such an ongoing

[30] For example, Tim Kaya (Vice President, United Healthcare Group) addressed the NCVHS Subcommittee on Standards Hearing on Operating Rules for Eligibility and Claim Status Transactions, July 21, 2010, indicating that

[31] CAQH CORE is a nonprofit alliance of health plans and trade associations that, among other projects contributing to administrative simplification has been developing operating rules for HIPAA transactions and code sets that are voluntarily being adopted.

program would help refine rulemaking, implementation, and enforcement strategies for the Privacy Rule. Likewise, developing methodologies and collecting baseline data for analyzing the effects of the transactions and code sets, adoption of uniform data standards, as well as privacy and security should be performed and made readily available to the public.

3.1 Financial and Administrative Standards for Transactions and Code Sets and Identifiers

In its advisory capacity to HHS and Congress on HIPAA, NCVHS will continue to hear testimony from stakeholders and make observations and recommendations relative to a variety of administrative simplification initiatives, including:

- **Operating rules** for health care claims, enrollment and disenrollment in a health plan, health plan premium payments, and referral certification and authorization transactions in accordance with ACA specifications.

- Implementation of a **health claims attachment** standard transaction and operating rules as specified in ACA.

- **Health plan certification** of compliance with the standards, regular review and recommendations for amendment of standards and operating rules, and assessment of penalties for health plans that fail to meet standards and operating rules requirements in accordance with requirements in ACA.

- Effectiveness of the current **change request process for standards** and finding ways to harmonize change requests among standards development organizations and operating rules authoring entities.

NCVHS identifies the following as areas from the HIPAA Administrative Simplification provisions that have not yet been addressed:

- **Acknowledgement transactions** (i.e., 997 or 999) are not mandated by HIPAA, but are used by willing trading partners. NCVHS is currently holding hearings to make applicable recommendations for facilitating and encouraging their use, if not mandating their use under the HIPAA provision for adopting "other financial and administrative transactions determined by the Secretary to be appropriate to improve the operation of the health care system and reduce administrative costs."

- **Electronic signature standard** was mandated for use in the HIPAA transactions and was to be developed by HHS in coordination with the Department of Commerce. Because none of the HIPAA transactions require a signature, an electronic signature standard has not been implemented. However, in light of several recent initiatives, it may be appropriate for NCVHS to play a harmonizing role with respect to electronic signature standards. Currently, the Interim Final Rule promulgated by the Drug Enforcement Administration on electronic prescribing requires enhanced authentication measures. The HIT Policy Committee and its Tiger Team as well as the HIT Standards Committee have made recommendations for authentication services to be included in Stage 2 M.U. criteria.

- **First report of injury standard transaction** was among the list of standard transactions in the HIPAA legislation, but has not been implemented nor is it called for in the ACA Administrative Simplification

provisions. There has been no demand for this standard transaction, primarily due to the fact that Workers' Compensation, the primary user of such a standard transaction, is not a covered entity under HIPAA.

- **Unique health identifier for individuals** in the U.S. was included in the HIPAA Administrative Simplification provisions to improve processing and recordkeeping in health care systems and transactions. Appropriation bills since 1999 have prohibited expending funds for its finalization until specific legislation calls for such a standard. Development of a unique health identifier may have important advantages for linking patient records. Such an identifier may protect privacy by avoiding the need to use other private information to achieve linkage. On the other hand, unique patient identifiers raise significant privacy concerns. Without support to explore these issues in light of new technologies and enhanced focus on care coordination, NCVHS cannot advise either HHS on the development of such policies or Congress on what legislative initiatives may be appropriate. However, NCVHS observes that HHS has proposed standards on a related issue, metadata for electronic health information exchanges in an Advanced Notice of Proposed Rule Making issued August 4, 2011.

Additional administrative simplification provisions in ACA section 1104 are outlined on a very aggressive timeline. NCVHS is tracking this timeline in making its recommendations for adoption of the following:

- Health plan identifier to be effective by October 1, 2012.
- Health care electronic funds transfer standard transaction, with an interim final rule by January 1, 2012 that is effective by January 1, 2014
- Operating rules for all standard transactions, with effective dates staggered over the period January 1, 2013 through January 1, 2016.
- Certification and periodic audits for health plan compliance with standards and operating rules for eligibility by a health plan, health claim status, health care EFT, and health care payment and remittance advice by December 31, 2013, and health claims, enrollment and disenrollment in a health plan, health plan premium payments, health claims attachments, and referral certification and authorization by December 31, 2015.
- Biennial review and recommendations for amendment of standards and operating rules, starting not later than April 1, 2014.
- Assessment of penalties for non-compliance with standards and operating rules requirements by a health plan not later than April 1, 2014.

CMS is tracking well against the timeline set forth in the legislation on its preparations for rulemaking. Nonetheless, adoption of the operating rules and other transactions will be very new for many providers and health plans – where the business case for their adoption must be made clear. NCVHS will continue to hold hearings and make recommendations relative to implementation and adoption of these standards.

ACA section 10109 also seeks input on the following:

- Electronic application process for enrollment of health care providers by health plans
- Whether HIPAA standards and operating rules should apply to health care transactions of automobile insurance, worker's compensation, and other programs or persons not described in HIPAA.

- Standard forms for financial audits required by health plans, Federal and State agencies, and other relevant entities.
- Transparency and consistency of methodologies and processes used to establish claim edits used by health plans.
- Publication of timeliness of payment rules by health plans.

3.2 Privacy and Security

Attention to privacy and security must be on "high alert" at all times. While many covered entities and their business associates are doing excellent work in this area, the fact that an organization does not distribute a notice of privacy practices or conduct a security risk analysis – just two examples of issues identified through complaints to OCR and private-sector surveys – remains of concern. Protecting privacy and security relates directly to the success of promoting EHRs and as a result, the success of achieving health and health care quality and cost improvements.

In addition, in considering the journey forward, it is important to remember that HIPAA applies only to covered entities and their business associates. Many other entities possess health information about individuals, in some cases having received this information from HIPAA-covered entities. Patients may not easily comprehend that the protections that apply to their health information in one context may not follow it to another.

- **Protection for Personal Health Records**. In 2006, NCVHS released its first of several letters on personal health records. Health Level Seven (HL7)[32] issued a Personal Health Record Functional Model in 2008. On August 17, 2009, the Federal Trade Commission (FTC) issued a Final Rule on Health Breach Notification that coordinated with the HHS Interim Final Rule on Breach Notification issued on the same date. However, at this point very little additional protections and privacy and security requirements are specifically applicable to personal health records offered to patients by independent, third-party vendors. This has created a significant disparity between the level of protection afforded to patient health information in electronic health records maintained by covered entities and the same health information when maintained in personal health records maintained by non-covered entities.

- **Preserving an appropriate degree of state variation in health privacy law without losing systemic interoperability continues to be a challenge.** This includes essential protections for privacy and confidentiality while harmonizing rules governing the nationwide health information exchange with the HIPAA Security and Privacy Rules and with other relevant federal regulations, including those applicable to substance abuse treatment and records. Several projects have been implemented over the past five years, including the Health Information Security and Privacy Collaboration (HISPC), which engaged 42 states in assessing current state privacy laws and the degree to which they represented barriers to electronic health information exchange. The project also established multi-state collaborations to find ways to address cross-state exchanges of health information and harmonization of state laws.

- **Developing a National Health Information Privacy and Security Framework for health information exchanges, and incorporating fair information practices** into the architecture of

the nationwide health information network, with applicable enforcement procedures and means to establish and maintain public trust.

NCVHS will be monitoring and potentially making recommendations relating to:

- Adoption of **modifications** to the HIPAA Privacy Rule, as mandated under HITECH, including new requirements for business associates and strengthening several of the protections surrounding disclosures of PHI.
- **Enforcement** of the HIPAA Privacy and Security Rules as new penalties, enforcement provisions, delegation of authority, and greater involvement in both enforcement and education at the State level have recently been mandated.
- **Breach notification** by both HIPAA covered entities (managed by OCR) and personal health record (PHR) vendors (managed by the Federal Trade Commission).
- The role of health information exchange and the nationwide health information network in care coordination and the emerging **accountable care organizations** and **bundled payments**.
- Updating regulations relating to handling **research data** as research now spans across multiple institutions and broader types of settings.
- **Personal health records, including** issues surrounding consumer confusion between EHR and PHRs and access to a patient's EHR and provider support for PHR.
- Individual control of **sensitive health information** accessible via the nationwide health information network for purposes of treatment with prompt notification if emergency access is obtained.
- **Metadata**. The development, identification and implementation of standards for the use of metadata with electronic health information
- **E-Discovery**. Standards to be used in the query and discovery of health information across systems.
- **E-consent**. Individual right to whether personally identifiable information is accessible via the nationwide health information network and to control access to and disclosures from such EHRs.
- **Network governance** based on participant privacy practices.
- **Effect of the Privacy Rule in banking**. In 2003, recommendations were made for HHS to address privacy in banking, an area that has been re-addressed as standards for electronic funds transfer under the Affordable Care Act of 2010 are being initiated.
- **Guidance on bringing medical equipment with information system components into compliance with the Security Rule**. In 2005, it was recommended that HHS provide guidance on securing the convergence between medical equipment and information. This may again surface as an issue as the Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) continues to conduct its review of regulating health information software, especially embedded in medical devices, and collecting adverse event reports.
- **Cloud computing** and the HIPAA Privacy and Security Rules.
- Data stewardship over **secondary uses** of health information, including for research, public health and surveillance.

3.3 Semantic Interoperability

NCVHS supports standards for semantic interoperability and stands ready to aid in addressing any gaps or issues related to adoption of such standards. As these may have the potential for expansion or

broader content standardization, NCVHS will monitor their utilization to determine what input may be required from its ability to hold public hearings and make legislative and regulatory recommendations.

In addition to addressing the issues of ICD crosswalks set forth under ACA, NCVHS will continue to monitor and make suitable recommendation regarding adoption of ICD-10-CM/PCS as part of the financial and administrative transactions as well as its incorporation in certified EHR technology.

3.4 Addressing the Journey Forward

The national movement toward the adoption of electronic health records, other health information technologies and health information exchanges underscore the value and benefits of HIPAA's Administrative Simplification provisions.

As noted throughout this report, the purpose of HIPAA's Administrative Simplification was to encourage the development of standards that would support an efficient and effective electronic health information system. Data standardization and protection are critically important as HIT, EHR and HIE have created significant needs and opportunities for increased convergence and integration between financial, administrative, clinical, and quality data and systems.

Information silos are being broken down. It is now very common to find physician offices with a fully integrated EHR that incorporates the practice management system (administrative operations). Providers of all types are increasingly using data warehousing and analytics functionality to determine the cost and quality (value) of the care they provide, especially as they prepare to participate in accountable care organizations (ACO) and other health reform initiatives. Health plans and public health agencies are developing 'electronic health record' representations of their individual-level health information. Health care in the provider setting has long been supplemented with case management and disease management from providers, but is now extending to care in the community, public health, and population health. A full integration of health information systems that include semantic, syntactic and operating interoperability, all within highly secured environments, that allows for longitudinal, cross-organizational integration of health records and support population health analysis will be the next paradigm.

As the creators of HIPAA envisioned, the efficiency and effectiveness of health and health care in the U.S. is improved through modern information technology use. Information technology also presents new challenges for privacy and security that require continued attention. This is the time for all stakeholders to ensure that the journey initiated with HIPAA goes forward with prudent but deliberate actions that rapidly and effectively achieve administrative simplification through compliance with health data standards. Ultimately, results are measured not only by implementation milestones, but also by realized tangible improvements throughout the health care delivery system. The journey forward includes many challenges, but represents immense opportunities.

Appendix A: NCVHS Statutory Reporting Requirements for HIPAA

The statutory reporting requirements from P.L. 104-191, Sec. 263. Changes in Membership and Duties of National Committee on Vital and Health Statistics include reporting on:

"A. The extent to which persons required to comply with part C of title XI of the Social Security Act are cooperating in implementing the standards adopted under such part.

B. The extent to which such entities are meeting the security standards adopted under such part and the types of penalties assessed for non-compliance with such standards.[33]

C. Whether the Federal and State governments are receiving information of sufficient quality to meet their responsibilities under such part.

D. Any problems that exist with respect to implementation of such part.

E. The extent to which timetables under such part are being met."

P.L. 104-191, Subtitle F – Administrative Simplification, includes requirements for adoption of the following standards:

- Financial and administrative transactions specified in the Act *and other financial and administrative transactions determined by the Secretary to be appropriate to improve the operation of the health care system and reduce administrative costs*.
- Code sets for appropriate data elements in the transactions.
- Unique health identifiers (ID) for employers, health care providers, health plans, and individuals
- Security standards (for health information).
- Electronic signatures, in coordination with the Secretary of Commerce, as may be needed in the transactions.
- Standards for the transfer of information among health plans for coordination of benefits.
- Timetables for adoption of initial standards and additions/modifications to standards.
- Penalties for failure to comply with requirements and standards.
- Penalties for wrongful disclosures.
- Effect of state law – that HIPAA supersedes contrary State law except with respect to any State law the Secretary determines necessary to prevent fraud and abuse, to ensure appropriate State regulation of insurance and health plans, for state reporting on health care delivery or costs, that addresses controlled substances, or relates to the privacy of individually identifiable health information that may be more stringent than a privacy regulation.
- That HIPAA does not apply to entities processing payment transactions by financial institutions.
- NCVHS changes in membership, with two appointed by members of Congress.
- NCVHS expansion of duties to include providing status reports and recommendations and legislative proposals to the Secretary and Congress related to the adoption of uniform data standards for and the electronic exchange of patient medical record information (PMRI).
- Recommendations to Congress to enact legislation on privacy of health information; and that if such legislation is not enacted within 36 months after enactment of HIPAA, the Secretary will promulgate final regulations containing standards for the privacy of individually identifiable health information (with preemption for State requirements that are more stringent.[34]

[33] The privacy standards were not referenced in this list of subjects because initially HIPAA called for privacy legislation and privacy regulation only if Congress failed to enact such legislation within three years.

[34] Congress did not enact privacy legislation by its self-imposed deadline. As a result, the Secretary promulgated a final Privacy Rule on December 28, 2000, with a modification published August 14, 2002 (effective April 14, 2003) after receiving many unsolicited inquiries and NCVHS holding hearings in August 2001 and January 2002.

Appendix B: Transactions and Code Sets

Financial and administrative transactions are conducted between health plans, clearinghouses, and those providers who conduct electronic transactions.[35] Transaction standards for enrollment in a health plan and premium payment are also available to any entity conducting such processes.

The following transaction standards are currently available for use:

Accredited Standards Committee (ASC) X12

270/271	Eligibility for a Health Plan (Inquiry and Response)
837	Claim or Equivalent Encounter Information (and Coordination of Benefits [COB])
276/277	Claim Status Inquiry and Response
835	Health Care Payment and Remittance Advice (Electronic Remittance Advice [ERA] and Explanation of Benefits [EOB])
278	Referral Certification and Authorization (Health Care Services Request for Review and Response)
834	Enrollment and Disenrollment in a Health Plan
820	Health Plan Premium Payment

National Council for Prescription Drug Programs (NCPDP)

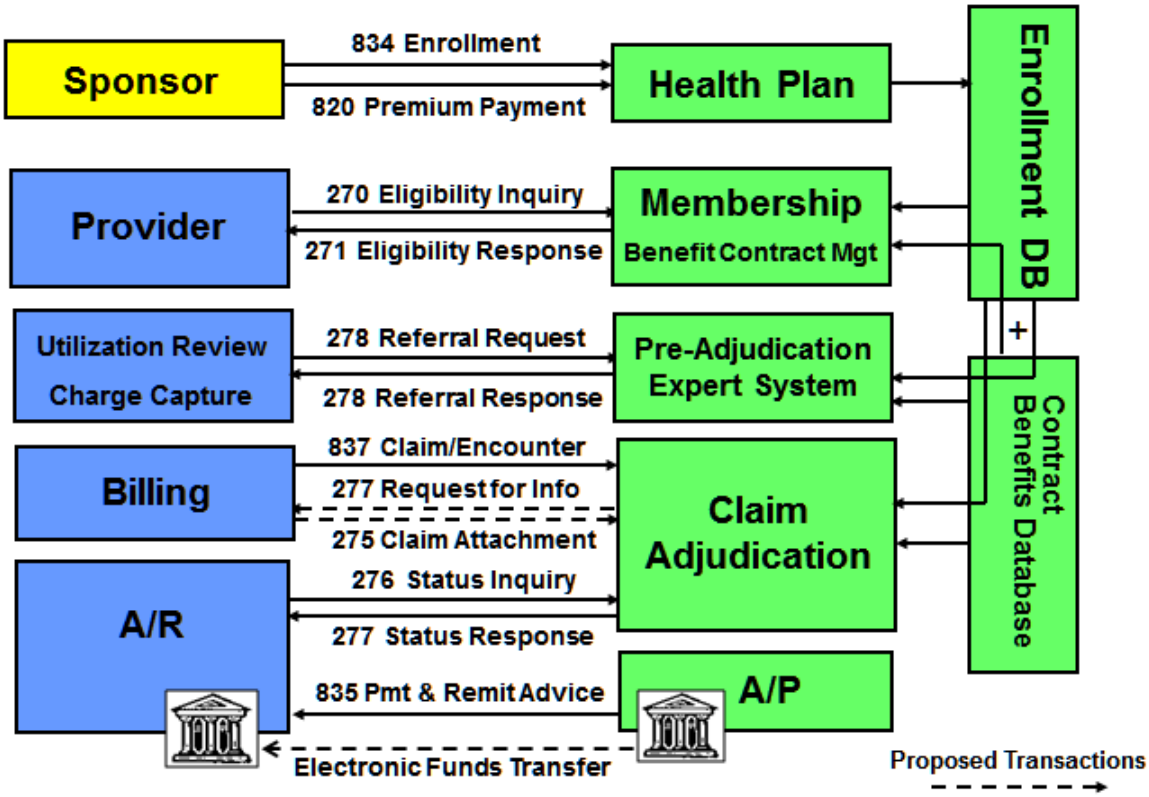
5.1 & D.0	Telecommunication and batch standards for claims. eligibility, and authorization
3.0	Medicaid pharmacy subrogation

HIPAA and ACA have required transactions for health claims attachments and electronic funds transfer that are currently in the process of being considered for adoption.

The following graphic illustrates the typical flow of the financial and administrative transactions in the non-retail pharmacy sector of health care. Those designated by number and name are from the ASC X12 standards development organization.

The retail pharmacy sector utilizes the ASC X12 835 Remittance Advice standard , but uses the National Council for Prescription Drug Program (NCPDP) standards for receiving formulary and benefits information from pharmacy benefits managers (PBMs), submitting claims, coordination of benefits, requesting an eligibility inquiry and receiving a response, and Medicaid subrogation. NCPDP also supports a Telecommunications standard.

[35] The Administrative Simplification Compliance Act of 2001 (ASCA) required all providers who submit claims to Medicare to use electronic transactions by October 16, 2003, except small providers or where a waiver for unusual cases has been obtained from the Secretary of HHS.


Sponsor
834 Enrollment
820 Premium Payment
Health Plan
Enrollment DB
Provider
270 Eligibility Inquiry
271 Eligibility Response
Membership
Benefit Contract Mgt
Utilization Review
Charge Capture
278 Referral Request
278 Referral Response
Pre-Adjudication
Expert System
+
Contract
Benefits Database
Billing
837 Claim/Encounter
277 Request for Info
275 Claim Attachment
Claim
Adjudication
A/R
276 Status Inquiry
277 Status Response
835 Pmt & Remit Advice
A/P
Electronic Funds Transfer
Proposed Transactions

Appendix C: NCVHS Congruence on Data Standardization and Legislative Initiatives

Legislation	Topic	Subcommittee on Standards	Subcommittee on Privacy, Confidentiality & Security	Subcommittee on Quality	Subcommittee on Population Health
	Focus:	(Data Standards, Interoperability, and Data Quality)	(Data Protection)	(Quality Data)	(Data Aggregation)
HIPAA	Transactions and Code Sets	X			X
	Medical Code Sets	X		X	X
	Patient Medical Record Information	X		X	X
	Identifiers	X	X	X	X
	Security		X		
	Privacy		X		
	Nationwide Health Information Network	X	X	X	X
	Enforcement	X	X		
HITECH	Breach (HHS)		X		
	Breach (FTC)		X		
	Privacy Modifications		X		
	Meaningful Use Incentives	X	X	X	X
	Business Associate	X	X		
MMA	E-prescribing (HHS)	X		X	
	E-prescribing (DEA)	X	X		
ACA	Operating Rules	X		X	
	Electronic Funds Transfer	X	X		
	Claim Attachments	X	X		
	Accountable Care Organizations	X	X	X	X

Appendix D: NCVHS Membership

CHAIR
Justine M. Carr, M.D.
Chief Medical Officer
Steward Health Care
Boston, MA

HHS EXECUTIVE STAFF DIRECTOR
James Scanlon
Deputy Assistant Secretary
Office of Science and Data Policy
Office of the Assistant Secretary for Planning and Evaluation, DHHS

EXECUTIVE SECRETARY
Marjorie S. Greenberg, M.A.
Chief, Classifications and Public Health Data Standards Staff
Office of the Director
National Center for Health Statistics, CDC

MEMBERSHIP

John J. Burke, M.B.A, MSPharm.
Vice President, Corporate Compliance Programs
Harvard Pilgrim Health Care, Inc.
Wellesley, MA

Raj Chanderraj, M.D., F.A.C.C.
Nevada Heart & Vascular Center
Las Vegas, NV

Bruce B. Cohen, Ph.D.
Director, Division of Research and Epidemiology
Bureau of Health Information, Statistics, Research and Evaluation
Massachusetts Department of Public Health
Boston, MA

Leslie Pickering Francis, J.D., Ph.D.
Distinguished Professor of Law and Philosophy
Alfred C. Emery Professor of Law
University of Utah
Salt Lake City, UT

Larry A. Green, M.D.
Professor and Epperson Zorn Chair for Innovation in Family Medicine and Primary Care
Department of Family Medicine
University of Colorado Denver
Aurora, CO

Mark C. Hornbrook, Ph.D.
Chief Scientist
The Center for Health Research, Northwest/Hawaii/Southeast
Kaiser Permanente Northwest
Portland, OR

Linda L. Kloss, M.A., RHIA, FAHIMA
President
Strategic Advisors Ltd
Chicago, IL

Vickie M. Mays, Ph.D., M.S.P.H.
Professor and Director
UCLA Department of Psychology & Health Services
Los Angeles, CA

Blackford Middleton, M.D., M.P.H., MSc
Corporate Director, Clinical Informatics, Research and Development
Chairman, Center for Information Technology
Partners Healthcare
Wellesley, MA

Sallie Milam, J.D., CIPP, CIPP/G
Chief Privacy Officer
West Virginia Executive Branch and West Virginia Health Care Authority
Charleston, WV

Len Nichols, Ph.D.
Director, Center for Health Policy Research and Ethics; Professor of Health Policy
College of Health and Human Services
George Mason University
Fairfax, VA

William J. Scanlon, Ph.D.
National Health Policy Forum
Washington, DC

W. Ob Soonthornsima
Senior Vice President, Chief Information Officer and Security Officer
Blue Cross and Blue Shield of Louisiana
Baton Rouge, LA

Walter G. Suarez, M.D., M.P.H.
Director, Health IT Strategy & Policy
Kaiser Permanente
Silver Spring, MD

Paul C. Tang, M.D.
Vice President and Chief Medical Information Officer
Palo Alto Medical Foundation
Mountain View, CA

James M. Walker, M.D., FACP
Geisinger Health System
Danville, PA

Judith Warren, Ph.D., RN
Christine A. Hartley Centennial Professor; Director of Nursing Informatics
KUMC Center for Healthcare Informatics
University of Kansas School of Nursing
Kansas City, KS