

# HIPAA Compliance: Where Are the Savings?

By Scott C. Withrow

---

## Table of Contents

1. [Introduction](#)
  2. [Electronic Transactions and Code Sets](#)
  3. [Privacy](#)
  4. [Security Requirements](#)
  5. [Where Are the Savings?](#)
  6. [HIPAA is Flawed](#)
  7. [Opportunity Exists](#)
- 

## Introduction

Think tank experts have long identified the administrative inefficiencies plaguing the U.S. health care system.<sup>(1)</sup> In November 1991, Secretary of Health and Human Services, Dr. Louis Sullivan, convened a forum of national health care leaders to discuss the challenges of reducing administrative costs in the U.S. health care system. The forum participants formed a voluntary, public-private task force called Workgroup for Electronic Data Interchange ("WEDI"), whose goal was to formulate an action plan to streamline health care administration by standardizing electronic communications across the industry. WEDI published reports in 1992 and 1993 containing detailed recommendations for standardizing electronic data interchange ("EDI") in health care.

Although delayed by the failed attempt at major health care reform during the first term of the Clinton Administration, WEDI recommendations were largely adopted when Congress included "Title II, Subtitle F-Administrative Simplification" in The Health Insurance Portability and Accountability Act of 1996 ("HIPAA").<sup>(2)</sup> The Administrative Simplification provisions of HIPAA seek to improve the efficiency and effectiveness of the federal health care system by encouraging the establishment of standards and requirements for the electronic transmission of certain health information. HIPAA mandates the development of standards in the following areas:

- electronic transactions (e.g., health claims, payments and certifications);
- code sets for data elements supporting electronic transactions (e.g., description of encounter, diagnosis, complications, etc.);
- unique health identifiers for patients, providers and plans;
- security standards; and
- electronic signature.

All standards were supposed to be consistent with the objective of reducing the administrative cost of providing and paying for health care.

Congress also recognized that the increased ease of transmitting and sharing individually identifiable health information had caused Americans to become more concerned about privacy and confidentiality issues. HIPAA mandates the development of concomitant privacy standards covering:

- personal rights regarding individually identifiable health information;
- procedures for the exercise of such rights; and
- authorized or required uses and disclosures of such information.

"HIPAA compliance" has come to mean compliance with the federal standards in the combined areas of electronic transactions, security and privacy.

After an extended rulemaking process with over 50,000 comments from the public, the Department of Health and Human Services ("HHS") eventually finalized regulations in some of the HIPAA areas.<sup>(3)</sup> HIPAA specifies that all affected persons must comply with the standards by October 16, 2002 for electronic transactions and by April 14, 2003 for privacy, except that "small health plans" with annual receipts of \$5 million or less have an additional 12 months to comply. Thus, all providers and large health plans must comply with the HIPAA's Administrative Simplification regulations commencing on October 16, 2002 for electronic transactions, and all affected persons should begin preparations for compliance immediately.

### **Electronic Transactions and Code Sets**

The regulations regarding electronic transactions and code sets seek to establish standards that facilitate electronic data interchange in health care. Currently, there are approximately 400 different formats used for electronic health care claims in the United States. Standard EDI format would permit data interchange between any parties without the need to program for multiple formats. HIPAA charges HHS with the task of developing standards for the following transactions: health claims, health encounter information, health claims attachments, health plan enrollments and disenrollments, health plan eligibility, health care payment and remittance, health plan premium payments, first report of injury, health claim status and referral certification and authorization.

### **Privacy**

In the waning days of the Clinton Administration, HHS issued massive final privacy regulations and explanation totaling 368 pages in the Federal Register. The privacy regulations impose major new administrative burdens on the health care industry, including the need for written patient consent for the use of health information, business associate agreements and patient rights to inspect and correct health records.

## **Security Requirements**

The proposed security regulations require all health plans and each health care clearinghouse and provider that electronically transmits or maintains health information to develop, implement and maintain appropriate security measures. In particular, all covered entities must encrypt electronic transmissions of health information. Again, the so-called Administrative Simplification regulations are imposing burdensome new administrative requirements on the health care industry. Regulators have committed to publish final security regulations by early 2002.

## **Where Are the Savings?**

Five years after the adoption of HIPAA, and ten years after the formation of WEDI, the entire health care industry still wonders: where are the administrative savings? The final privacy rule estimates net costs (not savings) of \$17.5 billion over ten years (2003-2012).<sup>(4)</sup> Industry estimates of the cost of HIPAA compliance exceed the government's estimates by up to six-fold.<sup>(5)</sup> The proposed security rule recognizes, but does not attempt to estimate, the significant costs to comply with the security procedures. HIPAA's only hope for achieving savings lies in standardization of electronic transactions.

Based on WEDI original estimates, HHS estimates that electronic processing would generate savings of \$1.00 per claim for health plans, \$1.49 for physicians and \$0.86 for hospitals. HHS assumed that electronic processing would grow with standardization, creating a total savings of \$29.9 billion over ten years (2002 to 2011), before the offsetting costs of implementing privacy and security protections. HHS admits that "[t]he increase in EDI claims attributable to HIPAA is highly uncertain and is critical to the savings estimate."<sup>(6)</sup> Hospitals already electronically process 88% of all health care claims and over 99% of all Medicare claims.<sup>(7)</sup> The bulk of the projected savings comes from increased electronic processing by physicians in groups of three or less, which currently process only 50% of their claims electronically.<sup>(8)</sup>

HIPAA compliance costs largely will be incurred in the early years and the benefits are projected to accrue in the later years. Regulators lengthened the cost-benefit analysis from 5 to 10 years in the final electronic transaction regulations because the net savings were negligible after only five years. Ten years is too long of a time frame for accurate prediction. In 1991, George W. Bush's father was still President, a personal computer running an Intel 80486 chip cost roughly \$10,000, and Tim Berners-Lee had just released the information distribution protocol called the World-Wide Web (WWW). The projected net savings of HIPAA compliance are speculative, at best.

## **HIPAA Is Flawed**

HIPAA suffers from two major flaws: obsolescence and complexity. HIPAA is based on the wrong technology model: an early-1990s world in which electronic health information was stored in large, centralized payer and provider legacy systems. HIPAA pre-dates the Internet explosion and broadband connectivity. Now providers and payers may store huge fields of data in a common cyberspace accessible with a telephone, cable or wireless connection.<sup>(9)</sup>

Both HIPAA and even Internet-based solutions fail to solve the fundamental cause of health care's administrative inefficiencies: the complexity inherent in the over-regulated, heavily managed, multi-payer, third party reimbursement system employed in the United States. HIPAA only standardizes transactions and code sets; it does not eliminate the need for providers to convert medical language into hundreds of code sets. Fraud and abuse monitoring requires manual processes, given the complexities and ambiguities associated with medical science.<sup>(10)</sup> HIPAA does nothing to cure the seemingly endless process of claims review, denial and re-submission that so infuriates providers and patients alike.

## **Opportunity Exists**

Payers and providers have an opportunity to use the HIPAA requirements as the basis for adopting a forward-looking information management platform based on extensible mark-up language ("XML"). The electronic transaction standards establish the foundation for creating uniform data tags that can be expressed in XML for all major health care transactions. XML permits the tagged data to be easily transferred and manipulated across computer platforms and over the Internet, if desired. XML provides a means of extracting just those data elements which would identify an individual, enabling the de-identified health information to be used for other purposes. With XML, special security procedures, such as encryption, can be focused on the individually identifiable data elements without having to encrypt the entire set of information.

Payers and providers are already devoting vast resources to comply with the requirements of the Medicare/Medicaid reimbursement system, health care insurers and other private payers. Many have recently adopted health care compliance programs in response to the government crackdown on fraud and abuse. Competitive pressures within the health care industry and limited government funding of health care constrain the additional resources that payers and providers can allocate to HIPAA compliance issues.

Providers and payers should proceed cautiously but deliberately during the HIPAA phase-in period. Technology is developing rapidly, particularly in the area of XML. In light of the speculative net benefits projected from HIPAA, providers and payers should implement only the regulatory minimum to comply with HIPAA rather than attempting to invent a grand scheme to solve all health care inefficiencies. As Internet-enabled technologies develop and prove to generate true administrative savings, the health care industry must be quick to seize the savings in order to fund HIPAA's costly privacy and security

procedures.

For more information, please see Scott Withrow's book entitled *Managing HIPAA Compliance: Standards for Electronic Transmission, Privacy, and Security of Health Information*, published by Health Administration Press, a division of the American College of Healthcare Executives. The book is available for sale and immediate download as an e book at <http://www.ache.org/pubs/ehipaa.cfm>. The printed version of the book can be ordered over the Internet at <http://www.ache.org/pubs/hipaa.cfm> or by phone at 301-362-6905.

Used with permission from *Managing HIPAA Compliance: Standards for Electronic Transmission, Privacy, and Security of Health Information* by Scott C. Withrow. (Chicago: Health Administration Press, 2001)

## **Endnotes**

<sup>1</sup> Goodman, John C. and Musgrave, Gerald L., *Patient Power*, Washington, D.C.: Cato Institute, 1992, excerpt appearing at <http://www.ncpa.org/w/w53.html>.

<sup>2</sup> Public Law 104-191, 42 U.S.C.A § 1320d *et seq.* (2001).

<sup>3</sup> <http://aspe.hhs.gov/admnsimp/pubsched.htm>.

<sup>4</sup> 65 Fed. Reg. 82462, 82761 (December 28, 2000).

<sup>5</sup> "One huge HIPAA," *Modern Healthcare*, December 18, 2000, page 8 (referring to a study funded by the American Hospital Association and performed by the First Consulting Group).

<sup>6</sup> 65 Fed. Reg. 50311, 50357 (August 17, 2000).

<sup>7</sup> 65 Fed. Reg. at 50356.

<sup>8</sup> *Id.*

<sup>9</sup> Cunningham, Rob, "Old Before Its Time: HIPAA and E-Health Policy," 19 Health Affairs 231, 232 (Nov./Dec. 2000).

<sup>10</sup> Kleinke, J.D., "Vaporware.com: The Failed Promise Of The Health Care Internet," 19 Health Affairs 57, 58-60 (Nov./Dec. 2000).

## BIOGRAPHY

Scott C. Withrow is a founding partner of Withrow, McQuade & Olsen, LLP, an Atlanta law firm, and author of *Managing Healthcare Compliance*, published in 1999 by Health Administration Press, as well as *Managing HIPAA Compliance*, published in 2001 by Health Administration Press. He structures legal relationships in healthcare, lectures to providers on compliance matters and practices general corporate law.

---

**©2001 Scott C. Withrow. All rights reserved.**

***NOTE: This site includes a summary of certain compliance issues facing healthcare providers today. This site does not, and is not intended to, give legal advice. Reference should be made to full text of statutes and regulations for complete analysis. Consultation with competent counsel is strongly recommended.***