
Administrative Simplification Part 2: The Not-So-Private Privacy Regulations

By Scott C. Withrow

Table of Contents

1. [Introduction](#)
2. [Background of Privacy Regulations](#)
3. [Free Use for Healthcare Treatment, Payment and Operations](#)
4. [Free Use for Other Government Interests](#)
5. [Prior Authorization Required for Marketing, Employment and Fundraising](#)
6. [Individual Rights to Inspect, Copy and Correct Health Information](#)
7. [Compliance Officer Gets Company](#)
8. [No Privacy From Whistleblowers](#)
9. [Compliance Costs](#)
10. [Conclusion](#)

Introduction

Last month's article, ["The Next Compliance Crunch: Administrative Simplification,"](#) suggested that the pending regulations on electronic transactions, code sets and security are far from simplifying. The concomitant proposed regulations on privacy are likewise complex, and largely fail to address legitimate concerns about preserving the privacy of individually identifiable health information.

Background of Privacy Regulations

Pursuant to "Subpart F-Administrative Simplification" of the Health Insurance Portability and Accountability Act of 1996, the Department of Health and Human Services ("HHS") proposed the so-called privacy regulations on November 3, 1999. The proposed regulations and explanation totaled 149 pages in the Federal Register. The regulations were intended to address increasing privacy and confidentiality concerns associated with electronic transmission and sharing of sensitive personal health information. A September 1999 Wall Street Journal/ABC poll found that Americans were more concerned about "loss of personal privacy" in the coming century than all other issues, including terrorism, world war and global warming.

Free Use for Healthcare Treatment, Payment and Operations

Health plans, clearinghouses and providers who transmit health information in electronic form ("covered entities") may use or disclose health information without individual authorization to carry out any treatment, payment or healthcare operations. The proposed regulations define "treatment," "payment" and "healthcare operations" very broadly.

"Treatment" means not only the direct provision of healthcare, but also the coordination of healthcare among providers (risk assessment, case management and disease management) and referrals from one provider to another. "Payment" includes all activities to obtain health plan premiums, determine coverage or obtain reimbursement for the provision of healthcare. "Healthcare operations" encompass:

- **Quality assessment and improvement activities, outcomes evaluation and development of clinical guidelines;**
- **Reviewing the competence of health care professionals, evaluating provider and health plan performance, and conducting training of health care students and trainees;**
- **Insurance rating activities, underwriting experience rating and reinsurance;**
- **Conducting medical review and auditing services, including fraud and abuse detection and compliance programs; and**
- **Compiling and analyzing information in anticipation of, or for use in, a civil or criminal legal proceeding.**

Free Use for Other Government Interests

The proposed regulations also permit use of health information, again without individual authorization, for various other quasi-governmental purposes:

- **Public health activities such as preventing or controlling disease;**
- **Health oversight activities of the federal health care system, including beneficiary eligibility and compliance with program standards;**
- **Judicial and administrative proceedings in response to a court or administrative tribunal;**
- **Coroners and medical examiners;**
- **Law enforcement purposes, including governmental intelligence, national security, and healthcare fraud;**
- **Governmental health data systems;**
- **Health care directives for incapacitated persons;**

- **Banking and payment processes;**
- **Research purposes;**
- **Emergency circumstances;**
- **Next-of-kin notification; and**
- **Armed forces uses.**

Prior Authorization Required for Marketing, Employment and Fundraising

The not-so-private regulations actually protect privacy in only a very limited number of situations. The proposed regulations require individual authorization before health information can be used for three main purposes:

1. **Marketing** - Use for marketing of health and non-health items and services by the covered entity, including sales or rentals of customer lists.
1. **Employment** - Disclosure to an employer for use in employment determinations.
1. **Fundraising** - Use or disclosure for fundraising purposes.

A study sponsored by the California HealthCare Foundation and published in January 2000 found that 19 of the top 21 health Internet sites already had privacy policies offering some limited protections on the use of an individual's personal information. However, the study found that most sites failed to follow their stated policies. The technological mechanisms behind the privacy violations included the use of "cookies," which track Web surfers' movements online, and banner ads, which in some cases can pick up information entered by visitors on the pages where they are displayed. Providers can easily avoid the marketing limitation in the proposed regulations by characterizing the information use as quality assessment and improvement activities, which are permitted without individual authorization. The proposed regulations fail to effectively address the public's legitimate concern about unauthorized disclosure of personal health information.

Individual Rights to Inspect, Copy and Correct Health Information

The proposed regulations do mandate certain individual rights relating to one's personal health information, although such rights have little to do with privacy. The regulations establish a right of individual access to personal health information, including the right to inspect and copy the information for so long as it is maintained, and to receive an accounting of all disclosures of protected health information (other than for treatment, payment and health care operations). Providers must act on such requests not later than 30 days following receipt of the request.

In addition, the proposed regulations provide the individual with the right to request a health plan or provider to amend or correct personal health information unless the covered entity determines that the information is already accurate and complete. Providers must act on correction requests within 60 days of the receipt of the request. The proposed regulations require covered entities to provide adequate notice to individuals of the policies and procedures for exercising their information rights. Regulators are again creating more cumbersome procedures that will force health care providers to expend more resources on tasks unrelated to medical care.

Compliance Officer Gets Company

Like the proposed regulations on security discussed in last month's article, the not-so-private regulations create detailed privacy requirements (see [Required Privacy Procedures](#)) that are analogous to the seven basic elements of a healthcare compliance program: written standards (Requirement 1), designated officer (Requirement 2), education and training (Requirement 3), audits and other monitoring (Requirement 4), internal reporting processes (Requirement 5), disciplinary mechanisms (Requirement 6) and investigation/remediation (Requirement 7). Over the last three years, federal regulators have added three new officers to the executive suite of a health plan or provider: the chief compliance officer, the designated security officer and the designated privacy officer.

No Privacy From Whistleblowers

The most outrageous proposal in the not-so-private regulations is to allow any member of a covered entity or a person associated with a business partner of a covered entity to disclose an individual's health information, without authorization, if such person believes that the information is evidence of a violation of criminal or civil law and the disclosure is made to: (1) relevant oversight agencies and law enforcement or (2) an attorney to allow the attorney to determine whether a violation of criminal or civil law has occurred or to assess the remedies or actions at law that may be available to the person disclosing the information. One can imagine a parade of medical records clerks hauling personal health files to the offices of their friendly plaintiff's attorneys to see whether they can share in the whistleblowers' jackpot. The regulations pervert an individual's right of privacy, fundamental to the United States and many state Constitutions, in favor of government financial interests under the whistleblower provisions of the False Claims Act.

Compliance Costs

The not-so-private regulations contain an interesting analysis of the estimated cost of compliance. Remember that these regulations are promulgated under the Administrative Simplification subpart of HIPAA with the declared objective of reducing the administrative cost of providing and paying for healthcare. According to the government's own estimate (see [Estimated Costs of Complying with the Proposed Privacy Regulations](#)), the five-year compliance cost of only not-so-private regulations (excluding the electronic reporting and security requirements of Administrative Simplification) will total a whopping \$3.775 billion, with the requirement to accommodate the amendment/correction of medical records accounting for 54% of the total five-year cost.

Regulators estimated that the cost of developing written policies required by the regulations would range from \$300 to \$3000 for providers, depending on the size and complexity of the provider, with the average being about \$375 (assuming provider associations develop standard policies usable by large numbers of providers). For health plans and clearinghouses, regulators estimate that development costs would range from \$300 for smaller plans to \$15,000 for the largest plans, with the average being about \$3050.

These compliance costs fall disproportionately on small entities in the healthcare sector. Small businesses, meaning entities having less than \$5,000,000 in annual revenue as defined by the Small Business Administration, account for 84.9% of all health care entities, over 91% of all physician offices and over 99% of all dentist offices. The regulations will further discourage primary medical service providers from engaging in their professions as small business persons because of the overwhelming administrative burdens in the healthcare reimbursement system.

Conclusion

The not-so-private regulations establish many administrative requirements but few substantive privacy protections to address the legitimate concerns of the American public. Government financial interests in constraining federal healthcare expenditures conflict with personal privacy desires. The administrative burdens of the proposed regulations are costly and fall disproportionately on small healthcare providers. Congress should legislate more effective and less costly privacy protections for healthcare information to address legitimate public concern in ways that are palatable to healthcare providers.

About the Author

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. He structures and documents legal relationships in healthcare, lectures to providers on compliance matters and practices general corporate law.

© 2000 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 the statutes and regulations for complete analysis. Consultation with competent counsel is strongly recommended.

