

## TELEMEDICINE REGULATORY ISSUE SUMMARY

### HIPAA's Privacy Rule Summarized: What Does It Mean For Telemedicine?

February 26, 2001

Author: *Glenn Wachter*

#### Contents

- Introduction to HIPAA
- Administrative Simplification
  - Reducing Administrative Overhead
  - Protecting Information
- Highlights on Health Information Privacy Rule
  - Certain Entities
  - Health Care Arrangements
  - Certain Information
  - Certain Transactions
  - Certain Information
  - Patients Must Give Consent
- First Steps To Compliance
- Implications for Telemedicine Encounters
- Conclusion
- Resources

#### Introduction

In 1996, Congress sought to streamline electronic medical record systems while protecting patients, improving health care efficiency, and reducing fraud and abuse. Passing Congress with bipartisan support, the Health Insurance Portability and Accountability Act (HIPAA, [Public Law 104-191](#)) became the legislative vehicle to address those issues. HIPAA is divided into seven standards, collectively referred to as Administrative Simplification. Since this law's passage in 1996, the [Department of Health and Human Services](#) (HHS) has published two major final rules, dealing with standards for electronic transactions and information privacy pursuant to [PL 104-191 Title II Subtitle F Sections 261-264](#). Due to the complexity of each final regulation, the highlights of the privacy rule will be discussed in this document as they relate to the practice of telemedicine and telehealth.

## **Administrative Simplification**

Administrative Simplification regulations deal mainly with two issues: 1) reducing the administrative overhead of health care entities; and 2) protecting individually identifiable health information in an increasingly electronic world. The [Federal Register](#) publication dates, as well as the compliance dates for health information privacy and electronic transaction standards are provided in Table 1 below.

### **Administrative Simplification Regulations Dates of Publication and Compliance**

1. Standards for Privacy of Individually Identifiable Health Information, Final Rule published 12/28/00, **Compliance Date: 4/14/03**; (2/04 for small health plans).  
See 45CFR 160-160.312 and CFR 164.102-164.534.
2. Standards for Electronic Transactions and Code Sets, Final Rule published 8/17/00, **Compliance Date: 10/16/02**.  
See 45CFR 160 and CFR 162.
3. National Standard Health Care Provider Identifier,  
See 63 FR 25272 and 25320.  
Proposed Rule published 5/07/98.
4. National Standard Employer Identifier,  
See 63 FR 32784.  
Proposed Rule published 6/16/98.
5. Security and Electronic Signature,  
See 63 FR 43242.  
Proposed Rule published 8/12/98.
6. National Standard for Health Claim Attachments,  
Proposed Rule not yet published.
7. National Standard Identifiers for Health Plans,  
Proposed rule not yet published.

### **Reducing overhead**

A considerable portion of every health care dollar is spent on administrative overhead. In health care, this overhead includes many tasks, such as: filing a claim for payment from an insurer; enrolling an individual in a health plan; paying health insurance premiums; and checking insurance eligibility for a particular treatment. These and other processes involve numerous paper forms, faxes and telephone calls, and many delays in communicating information among different locations. Such activities affect everyone involved in the health care system. They include health plans that process insurmountable

mounds of paper forms that differ in content from one plan to another, and health care practitioners who bill multiple health plans with their varying forms and formats. Administrative logistical nightmares like these create higher costs for health care providers, health plans, and are passed on to purchasers of health care, such as consumers, the government, and employers. That is why a key purpose of HIPAA's ASR is to reduce these burdens through streamlining and standardizing health care operations as much as possible from one health care entity to another.

### **Protecting information**

Protection of patient privacy is a second major focus of ASR, and the chief focus of the rule summarized in this article. According to Janlori Goldman, Director of Georgetown University's [Health Privacy Project](#), "Americans are increasingly concerned about the loss of privacy in every-day life, and especially for their health information. The lack of privacy has led people to withdraw from full participation in their own health care because they are afraid their most sensitive health records will fall into the wrong hands, and lead to discrimination, loss of benefits, stigma, and unwanted exposure. Protecting privacy will help to improve health care in this country." Goldman calls HIPAA "the most sweeping privacy law in U.S. history<sup>i</sup>."

To better understand the drive behind protecting health information, consider a few statistics from recent polling.

- 1 in 5 Americans believes that a health care provider, insurance plan, government agency or employer has improperly disclosed personal medical information<sup>ii</sup>.
- 72% of those polled believed that their medical information had been improperly disclosed. Almost a third of health care leaders could describe confidentiality violations in their organizations in detail<sup>iii</sup>.
- 76% of online users in very good or good health are very concerned that their health insurer will use information that they provide online to a Web site to limit or affect their coverage<sup>iv</sup>.

### **Highlights of Health Information Privacy Rule**

The privacy rule has been applied very broadly to entities that transmit certain information in the course of various health care operations or financial/administrative transactions. Chances are that if an organization contacts patients and is involved in the transmission of their health information, this rule will impact its operations in some way. Some of the basic and critical concepts are described below<sup>v</sup>.

#### **Certain entities**

Health plans, health care clearinghouses (translate health care data into a usable form to secure payment), and health care providers that transmit 'protected health information' in electronic or paper form in connection with a 'standard transaction' are subject to the provisions of this rule. Health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or hospital, transmit electronic transactions on their behalf. Providers also cannot circumvent these rules by assigning a non-covered entity the task, such as a business

associate, because by association with a covered entity, the business associate is also bound by these rules.

The final rule broadens the privacy rules to business associates of covered entities, requiring them to maintain a contract with such associates with whom they share protected health information. Likewise, a business associate contract is required if protected information is received or created on behalf of covered entities. Covered entities are required to report privacy violations of their business associates, and must take appropriate corrective action.

### **Health care arrangements**

Covered entities that operate as "organized health care arrangements" may share protected health information for the operation of such arrangement without becoming business associates of one another. Similarly, covered entities do not become business associates of one another if sharing protected health information for purposes of providing treatment.

### **Certain information**

Individually identifiable health information in any form or medium is considered by ASR to be 'protected health information.' This information includes: 1) Name and address; 2) Date of birth; 3) Social security number; 4) Payment history; 5) Account number; and 6) Name and address of the health care provider and/or health plan.

In a marked departure from the proposed rule, the final HIPAA privacy rule applies to individually identifiable health information that is maintained in any for or medium, including electronic, paper, and oral. While this means that even small health care entities cannot escape ASR<sup>vi</sup>, it does provide one unified standard to be applied evenly across all health care organizations, rather than having different regulations for electronic records and another for paper. According to former HHS Secretary Donna Shalala, "We originally thought we would just do electronic records, but the fact is, all the paper records are being transferred to electronic records." Having two rules could possibly preventing them from adopting electronic record technology that would in the long run be beneficial to their health care operations.

### **Certain transactions**

When protected health information is transmitted outside of the course of direct patient treatment, but in administrative circumstances, privacy rules specify how protection by covered entities is to be met. Use or disclosure of protected information in the following financial or administrative transactions, termed "standard transactions," requires the consent and in some instances more formal authorization by the patient. Standard transactions include the following:

- (1) Health care claims or equivalent encounter information.
- (2) Health care payment and remittance advice.
- (3) Coordination of benefits.
- (4) Health care claim status.
- (5) Enrollment and disenrollment in a health plan.
- (6) Eligibility for a health plan.

- (7) Health plan premium payments.
- (8) Referral certification and authorization.
- (9) First report of injury.
- (10) Health claims attachments.
- (11) Other transactions that the Secretary may prescribe by regulation.

**Patients must give consent**

Health care providers, as covered entities, must comply with the privacy rule when they are engaged in a 'direct treatment' relationship with the patient whose protected health information is used or disclosed. This amounts to requiring that physicians obtain a patient's 'consent' before using or disclosing his or her health information. In the proposed rule, HHS eliminating patient consent forms for routine purposes. However, in its review of 52,000 comment letters, HHS was persuaded to maintain the current practice employed by most practitioners and providers of obtaining advance written consent for routine disclosures. Additionally, the proposed rule limited practitioners to only use or disclose the minimum amount of protected information necessary. However, the final rule gives providers discretion in determining which health information to include when sending patients' medical records to other providers for treatment purposes.

Other covered entities need not ask for this consent as long as the purpose for using or disclosing the protected information can be considered for the purposes of treatment, payment or health care operations. Time-limited, specific authorizations are needed for non-routine disclosures, such as life insurance or marketing. 'Written authorization' must be obtained from the patient for any other kind of use or disclosure, with few, however appropriate exceptions (law enforcement purposes, public health, use by coroners, etc.).

**First steps toward compliance**

Education of each health care entity's leadership is an obvious and necessary first step, since this group must interpret how an organization is situated in the health care system, and is responsible for initiating strategic planning. Getting the medical leadership on board since compliance will undoubtedly require substantial investment up front, but may have a significant return on cost savings in the long run.

A compliance officer must be identified, who will guide the organization through this process. Since the very essence of the privacy rule involves relationships—between hospitals, billing offices, health care providers, health plans and patients—in which protected health information is transmitted, this officer ought to carefully examine organizational interactions. He/she must determine the possible exposures for the organization in which patient information is used or disclosed. The first work of the compliance officer amounts to a detailed intra- and inter-organizational assessment of present and future transmissions of protected health information.

In general, priorities must be made, including timelines, budgets, and staff estimates for addressing the assessment's findings. Some suggest that instead of investing heavily in HIPAA regulatory assessments—likely the bread and butter of many new HIPAA consultants—they should instead be examining industry best practices models and applying that infrastructure to their organization. Steering the organization to adopt a model of best practice for information

security might, some suggest, be the best first step. If the organization is already at that point, then a detailed assessment may be in order.

### **Implications for telemedicine encounters**

Because by its very nature, telemedicine means that protected health information can potentially be sent anywhere in the world in a matter of seconds (your results may vary), the red privacy flag seems to be raised. Telemedicine consults typically include a variety of protected health information about the patient. An electronic medical record may be included in the real-time or store-and-forward transmission, or some other kind of attached file may contain most kinds of protected data. One could easily imagine the shuttling of social security numbers, names, addresses and medical conditions to a distant medical center. After the distant provider renders his or her consultation, the patient's information could be sent any number of places or left carelessly on the telemedicine workstation for other unauthorized parties to discover. There appears to be some opportunity for improper use of such important patient information.

The final rule requires health care providers to obtain consent prior to using or disclosing protected health information to carry out treatment, payment or other health care operations. To the best of the author's knowledge, such consent is already a common part of in person health care, and the consent device is routinely used—albeit for different purposes—in telemedicine encounters. Additionally, since the consulting provider is most likely a physician, there is already the underlying assumption that this information is already deemed confidential as a matter of ethical code of conduct. It may be others who may come into contact with this protected information that we ought to be concerned about. What happens to patient information when the consultation has concluded? It is true that where protected information is headed and who will be review it must be clearly determined and authenticated by some means. The patient must be made aware, and give his or her consent that such a transmission is permissible as a necessary disclosure in the course of treatment.

It is worthwhile to determine whether or not a consulting practitioner will be interacting with the patient directly or indirectly. Indirect practitioners would include radiologists and pathologists, who provide health care services for patients indirectly, through the orders of another health care provider. Other store-and-forward<sup>vii</sup> applications of telemedicine may be looked at in a similar fashion.

### **Conclusion**

[Health Data Management](#) reported on February 20, 2001 that the final privacy rule's effective date would be delayed from February 26, 2001 to April 14, 2001 because of a paperwork glitch. According to the story, Clinton Administration officials confirmed that they failed to transmit the final rule to Congress and the Government Accounting Office (GAO) when it was published. AHA officials concede that while this glitch is unrelated to their bid for reopening the rule, this delay would give them more time to make their case. This means, barring any further executive or administrative delays that the final compliance date for the privacy rule is April 14, 2003 (and 2004 for small health plans).

## TELEMEDICINE REGULATORY ISSUE SUMMARY

HIPAA Privacy Rule Summarized: What does it mean for telemedicine?

Glenn Wachter

Page 7

3/22/01

---

This rule can be expected to be a heavy financial burden to many health care entities, even though the overall intent is actually to save money by streamlining ways in which health care organizations interact. Some experts anticipate the cost of implementing HIPAA will exceed that of preparing for Y2K. Of the nine parts of the [Administrative Simplification](#) in HIPAA, HHS has projected the privacy rule alone to cost health care institutions \$17.6 billion (19 cents per health care visit) over the next ten years<sup>viii</sup>. The [American Hospital Association](#) argues that this is a cost that many health institutions cannot afford and may push them to the brink of closing their doors.

Privacy advocates are generally pleased, with a few exceptions where loopholes have been provided and the unusually broad definition of 'health care operations.' Some loopholes in the final rule may give health plans free reign to use protected health information for corporate purposes like marketing without first securing patient consent or authorization. For health care practitioners, protecting patients' privacy is not a new concept, however, now every category of covered entity must now play by the same rules.

Overall, the privacy rules don't seem to be significantly different from the way in-person medicine, or telemedicine for that matter, is already practiced. That said, focused attention and tracking of where protected information is sent and who uses it should be expected. At this point, the numerous HIPAA regulations—the final privacy rule in particular and other rules yet to be promulgated—will have a great impact on the financial and administrative activities of health plans, billing offices, hospitals and health data clearinghouses.

### Learn more

- HHS's Administrative Simplification Page <http://aspe.os.dhhs.gov/admsimp/index.htm>
- Department of Health and Human Services <http://www.hhs.gov/>
- American Hospital Association Model Privacy Notice <http://www.aha.org/hipaa/resources/Content/ModelPrivacyNotice.doc>
- AHA has created a 9-page model privacy notice for hospitals, based on the final medical privacy rule. A model consent form (three paragraphs) is also available.
- Health Privacy Project, Georgetown University <http://www.healthprivacy.org/>
- Arent Fox <http://www.arentfox.org/>
- Joint Healthcare Information Technology Alliance <http://www.jhita.org/admsimp.htm>
- Electronic Privacy Information Center <http://www.epic.org/>
- Siemens HIPAA Central <http://www.smed.com/hipaa/index.php>
- Health Data Management HIPAA Resource Guide <http://www.healthdatamanagement.com/html/Guide/List.cfm?GuideCatID=41>

## **Bibliographic citations**

---

<sup>i</sup> Remarks of Janlori Goldman, Director, Health Privacy Project. December 20, 2000. Institute for Health Care Research and Policy, Georgetown University. ([http://www.healthprivacy.org/usr\\_doc/43840.doc](http://www.healthprivacy.org/usr_doc/43840.doc)).

<sup>ii</sup> Princeton Survey Research Associates poll conducted for California HealthCare Foundation, 1999.

<sup>iii</sup> Louis Harris & Associates survey conducted for Equifax, 1992.

<sup>iv</sup> Cyber Dialogue poll conducted for California HealthCare Foundation and Internet Healthcare Coalition, 2000.

<sup>v</sup> HHS's final rule for privacy of health information is a lengthy document, totaling 369 pages of federal regulations, rules and definitions. Some of the highlights of this rule are provided below, but it should be evident that this is only a summary and not meant to be comprehensive or inclusive of all the detailed provisions. (Readers interested in reviewing the entire privacy rule should see the 'Resources' section below.)

<sup>vi</sup> The compliance deadline has been extended by one year (April 14, 2004) for smaller health plans, giving them a longer time period to fulfill HIPAA's privacy rules.

<sup>vii</sup> Captured still images, audio or video clips, or data that are transmitted or received at a later time (sometimes no more than a minute). Teleradiology and teledermatology are two examples of this type of telemedicine interaction, where the referring practitioner sends and consultant reviews a patient's medical data at different times.

<sup>viii</sup> HHS Issues Final Privacy Rule. January 2001. Arent Fox Web site.