California Association of Homes and Services for the Aging

Legal Update

May 2001

HIPAA: AN INTRODUCTION

By Allan D. Jergesen, Esq., Hanson, Bridgett, Marcus, Vlahos & Rudy, LLP

Since the end of 2000, anyone connected with the health system has been bombarded with information about the HIPAA rules and their potentially dire consequences. Scarcely a week goes by without an announcement from Washington about what the Bush Administration will be doing with HIPAA. Meanwhile, consultants warn audiences that they must prepare for an entirely new scheme of regulation based on the need to preserve the confidentiality of electronic health information. It is suggested that businesses must position themselves now to comply with what will be new and onerous requirements. Not surprisingly, those who administer retirement facilities are at a loss regarding whom to believe and what to do.

The purpose of this article is to give CAHSA members a general introduction to HIPAA. In this vein, it will explain the background of the HIPAA legislation and explore the context in which the HIPAA rules will operate. It will also summarize the various areas that HIPAA addresses, of which the privacy rules are but one aspect.

The Origins of HIPAA

"HIPAA" is an acronym for the Health Insurance Portability and Accountability Act of 1996. As its name suggests, the Act dealt primarily with the portability of health insurance plans covering employees who are switching jobs. The main purpose of Congress was to ensure that workers who transfer employment can take their health insurance with them and to establish rules under which they might do so. But the Act also touched on a number of other areas, including the creation, retention, and transmission of electronic health information. Congress felt that the time had come to reduce the administrative cost of providing health care by making it easier to transmit and use medical information in electronic form. To accomplish this, it declared its intention to create national standards for the use and transmittal of electronic materials.

Congress realized, however, that it was unlikely to be the most suitable vehicle for establishing standards. The rules would have to be technical and detailed, requiring input from computer experts, information specialists, industry associations, and consumer groups. Accordingly, it stated that, if it did not create standards by a certain time, the federal Department of Health and Human Services was to act through the administrative rule making process. This is exactly what has occurred, as the Department has promulgated various sets of regulations governing electronic health information. Each set of regulations is considered to be "HIPAA rules." However, each affects providers of health and related services in markedly different ways.

Electronic Transmission and Identifier Rules

The Department's first step was to propose standards for the transmission of electronic information that would apply across the country to everyone engaged in such transactions. To this end, it proposed rules in 1998 that prescribed standardized formats for electronic data exchange ("EDI"). These rules became final in August, 2000 and must be complied with by **October 17, 2002**. The rules identify certain standard health care transactions that are likely to involve the exchange of data in electronic form. One such transaction, for example, is the making of a claim by a provider to a payor for reimbursement. The rules then prescribe the exact information that must be included in such transactions by reference to various "code set" standards that already have been prescribed by public or private bodies. As a result, those involved in the electronic transmission of medical information will know for the first time exactly what information must be provided and what information must be received. This will give everyone a common language for exchanging information.

By October 17, 2002, then, health providers and others will have to be able to run standardized transactions and to transmit data in standardized forms. Since they are unlikely to have the technical knowledge themselves, providers will have to rely on manufacturers of hardware and software systems to embody the new standards in their products. This is similar to what happened with the Y2K issue. Rather than asking whether a system on the market is "Year 2000 Compliant," the provider will have to ask whether it is "HIPAA EDI Compliant." As an alternative, providers

may retain so-called "health care clearinghouses," whose function will be transmit their incoming and outgoing data into HIPAA-standardized transaction formats. Although this will bring another party into the mix, it may be more cost-effective in the long run than trying to use in-office systems to put electronic material in a HIPAA-compliant standardized format.

A second set of HIPAA rules involves proposed "national identifiers." These have the straightforward purpose of providing unique codes for designating individual players in the health care system. Thus far, national identifier rules have been proposed for health care providers and employers. They will eventually be proposed for health care payors. The Department is shying away, however, from proposing them for patients. While national patient identifiers might make sense from the perspective of efficiency, there is concern that the public will not accept them until it is more comfortable with the electronic transmission of identifiable health care data on a wide basis.

Security Rules

Even as they have moved to streamline the transmission of electronic health information, Congress and the Department have appreciated that they may be creating a new problem: with the increase in efficiency, information becomes more easily accessible to a wide variety of people in a wide variety of places. The chances for improper disclosures rise markedly, as does the potential harm that may result. Recognizing these concerns, Congress directed the Department to create so-called "security" and "privacy" rules to govern the use and transmission of electronic health information in the absence of Congressional action. Since Congress has not acted thus far, the burden has rested with the Department.

"Security" refers to the protection of information systems against unauthorized access, modification, or destruction. The goal is to ensure that electronic health information is maintained in a safe and secure manner, and that it is used and disclosed only in a conscious and responsible way. In August, 1998, the Department proposed security rules for electronic health information. These ultimately will have a profound effect on how providers operate medical record departments and maintain health information systems. In essence, they will require providers to establish clear administrative procedures to protect electronic information, including training employees, maintaining the security of work stations, and screening hardware and software to ensure that they include adequate features to prevent unauthorized access. In addition, providers will have to establish physical safeguards to protect their computer systems, including mechanisms to shield them from natural catastrophes such as fires or earthquakes and off-site backup systems to preserve data. They also will have to create "technical" security services such as special identifiers that will limit access to information and audit programs that trace and identify instances of improper access. Finally, providers will have to create security mechanisms to guarantee that electronic information is transmitted properly, such as schemes for encrypting material and programs for ensuring that electronic information is received in the same way that it is sent out. The security rules are still in proposed form and, as with the other rules, will prescribe a lead time of two years between the date that they become final and the date on which they must be complied with.

Privacy Rules

Most of the attention that HIPAA has received in recent months concerns the so-called "privacy" rules. These set forth standards that providers and others will be required to follow when disclosing medical information to outsiders. The Department first published the privacy rules in proposed form in November, 1999. To its surprise, the draft attracted over 50,000 comments. On December 28, 2000, in its final days in office, the Clinton Administration published the rules in final form with much fanfare. After taking office in January, 2001, the Bush Administration delayed the effective date of the rules and added a 30-day comment period that ended on March 30, 2001. During that time, the Department received 24,000 additional comments. Many of the commentators questioned the length and complexity of the rules. Among them were organizations representing hospitals, physicians, nursing facilities, and other health care providers that questioned the feasibility and costs of compliance. On the other side were consumer and privacy advocates who argued that the time had come for national confidentiality standards. After considering the various arguments, the Secretary of the Department announced that the rules would become final on April 14, 2001, as scheduled. The actual compliance date then would be April 14, 2003. The Secretary suggested that there almost certainly would be extensive changes to the rules prior to the compliance date, targeting certain requirements that seem particularly burdensome to providers. In the event that there are changes, the compliance date most likely will be pushed further into the future.

As of now, however, the privacy rules will become enforceable in less than two years. Anyone who is potentially affected is therefore advised to understand their overall scope and to begin considering mechanisms for compliance. Subsequent Legal Updates will explain the exact applicability of the rules to CAHSA members. They also will suggest what CAHSA members can do now to begin the compliance process, while avoiding an overcommitment to any particular course at this relatively early date.