White Paper

Salu, Inc.
4160 Douglas Boulevard
Granite Bay, CA 95746
Phone: 916.789.4160
Fax: 916.789.4159

Understanding HIPAA – A Brief Overview for Medical Practices

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was designed to establish standards and requirements for electronic transmission and storage of certain healthcare information used by healthcare providers, health plans and business entities involved in healthcare. The main purposes of HIPAA are:

1. To allow patients to carry insurance coverage to different plans if they change employment (portability).
2. To establish uniform standards for electronically stored and transmitted healthcare data.
3. To improve efficiency of sharing health information among entities involved in healthcare.

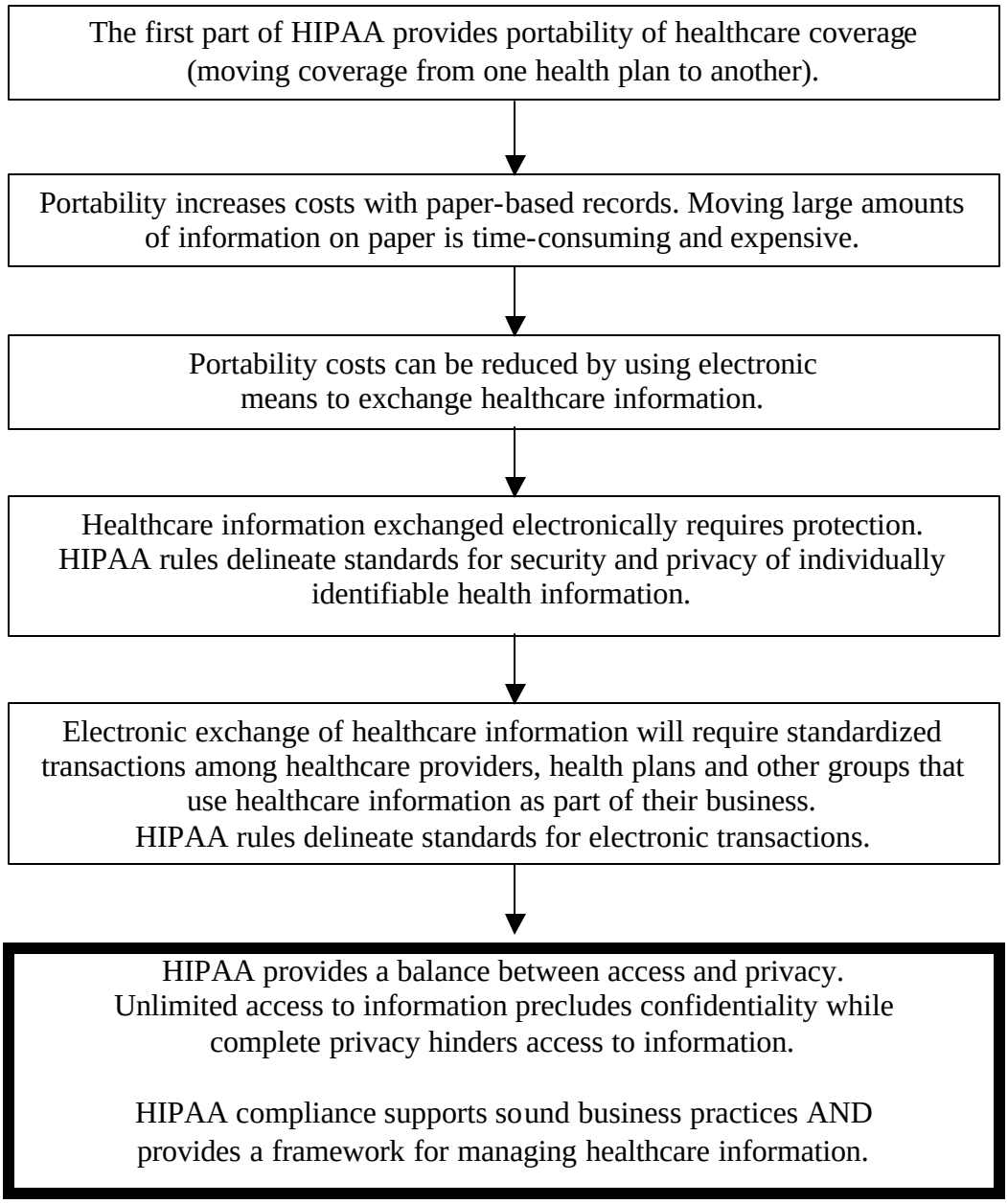
Administrative rules, which are intended to reduce costs and lift administrative burdens by standardizing electronic health information transactions, are being introduced as part of the HIPAA mandate.

Authored by: Jay Eisenberg MD

Privacy, Confidentiality and Security Terminology

- Privacy is the right to be left alone and refers to individual control over the use and disclosure of information.
- Confidentiality is the status accorded to information that indicates it is sensitive and should be protected.
- Security refers to the administrative, technical and physical safeguards that protect a system and information against unauthorized disclosure.

The logic behind the HIPAA administrative rules is illustrated below:



Authored by: Jay Eisenberg MD

Privacy, Confidentiality and Security – The Salu Perspective

The many components of the HIPAA administrative rules are at different levels of review. The most complex and probably the most important set of HIPAA rules are the "Standards for Privacy of Individually Identifiable Health Information." These proposed rules were made public in November 1999. After extensive public comment and a delay of six weeks to gather even more public comment, the final privacy rules became effective on April 14, 2001. The good news is that healthcare providers will have 24 months to become compliant with the new rules. For the privacy rules, healthcare providers will have until April 2003 to become compliant.

The final privacy rules broadened the scope of what information is covered. Individually identifiable health information, regardless of the form or format in which it is maintained or transmitted, is covered. The initial proposed regulation covered only health information that had been electronically maintained or transmitted. Products and services provided by Salu will be affected by the HIPAA privacy rules. To prevent unauthorized use of personal healthcare information, all healthcare data transmitted across the Internet should be encrypted. Although HIPAA does not specify a level of encryption, Salu Websites and services are equipped for 128-bit encryption, currently the most secure level. However, anyone accessing Salu services must also be using an Internet browser that supports 128-bit encryption to ensure that this level of encryption is maintained. AOL, Netscape and Internet Explorer version 4.0 or higher support 128-bit encryption.

Privacy, Confidentiality and Security – The Provider Perspective

The HIPAA privacy standard applies to individually identifiable health information that is transmitted or maintained in any form or format. The final HIPAA privacy rules answered an important question that was raised in regard to the day-to-day management of personal healthcare information: How can one determine if information has been or will be electronically stored or transmitted?

The answer is that it is not necessary to determine whether the information has ever been in an electronic format. It will be easier from a practice standpoint in that all personal healthcare information in the medical records is covered under HIPAA and will have to be protected.

As the HIPAA administrative rules become effective, it will be the responsibility of healthcare providers to have processes and procedures in place so that they are compliant with all regulations. Medical practices will have 24 months to comply with each set of rules as they go into effect. To be compliant with privacy and security rules, providers will be responsible for:

1. Planning for emergencies, including periodic backup of data, critical facilities availability and disaster recovery procedures.

Authored by: Jay Eisenberg MD

2. Determining level of access to healthcare information and providing training to all practice staff members about privacy and security procedures.
3. Designating a privacy official to oversee the confidentiality and security procedures. Fulfilling this requirement would not necessarily require hiring a new employee whose only responsibility is security and confidentiality. Designating an existing employee (e.g., practice manager) as the privacy officer should suffice.
4. Implementing physical safeguards to prevent unauthorized access. Securing workstations and storage media (e.g., diskettes) in a locked room or closet, keeping records of authorized access and implementing workstation policies including automatic logoff, regular backup of data and storage of backup media will be required.
5. Maintaining written policies and procedures that document compliance of HIPAA rules and making these available to all personnel. These written formal policies cover all aspects of HIPAA rule compliance and will probably be extensive.
6. Implementing chain of trust agreements with partners with whom the practice exchanges healthcare information. Also, policies for sanctions against staff and business partners who fail to comply will have to be documented.

This list is not inclusive but delineates some of the areas critical for HIPAA compliance relating to small group practices.

HIPAA and Patient Authorization

Virtually all of the uses of the healthcare information used for the usual practice of medicine within a medical practice will not require specific patient authorization. The use of personal patient information for marketing and fundraising is a different issue. A medical practice would be required to contact a patient and allow them to 'opt out' from disclosure of their information. This area of the final privacy rules still has loopholes.

HIPAA Compliance

Because all of the final HIPAA standards have not been published, neither Salu nor any healthcare-related business can be "HIPAA compliant" today. We feel it would not be honest to imply to our Members that Salu is HIPAA compliant. Salu currently employs the highest level of security to protect confidentiality of healthcare information and is in compliance with all current legal and regulatory requirements. Salu employs encryption levels that are the highest available, and all Patient Care forms exist on our secure server.

Similar to a medical practice, Salu will have 24 months to become compliant with the HIPAA rules. We have already initiated a complete review of our

Authored by: Jay Eisenberg MD

security and confidentiality policies and procedures. Salu fully intends to become compliant with the HIPAA rules as they are put into effect.

Salu Member Service Commitment

Salu feels that patient privacy and health information confidentiality are cornerstones of the physician-patient relationship. Salu is committed to supporting the trust that physicians develop with their patients by developing products and services that maintain the secure and trusting relationship physicians strive for with their patients. We have added a new section called Manage Your Practice available in the Member Center. Among many of the topics covered in Manage Your Practice is HIPAA and how it affects medical practices. Also provided are tools for designing and implementing a compliance program. We encourage you to contact Member Services at 1-888-288-7258, Monday-Friday, 8 am-5 pm Pacific Standard Time. Or, e-mail support@salu.net with questions you may have about HIPAA or any Salu products or services.

Authored by: Jay Eisenberg MD
Chief Medical Advisor, Salu, Inc.
Clinical Associate Professor, Medical Informatics
Clinical Professor, Pediatrics
Oregon Health Sciences University