

MEMORANDUM

TO: International SPA Association ("ISPA") Membership
FROM: International SPA Association
DATE: October 1, 2003
RE: HIPAA and Your Company

I. Background

This Memorandum provides information on the federal standards for safeguarding the privacy of individually identifiable health information to which certain ISPA members have access. As you may already know, the Department of Health and Human Services ("HHS") issued regulations¹ under the Health Insurance Portability and Accountability Act of 1996² (collectively, "HIPAA"). The HIPAA rules, which became effective April 2003, apply to all "Covered Entities," defined as health plans, health care clearinghouses and health care providers that transmit any health information in electronic form in connection with a list of specified transactions.³

Essentially, HIPAA's sweeping health information privacy rules are designed to ensure the protection and security of medical records and other personal health information, and to protect an individual's right to privacy in matters involving their health care. Specifically, HIPAA's requirements relate to the use and disclosure of protected health information ("PHI")⁴ by Covered Entities. PHI generally may not be used or disclosed unless the disclosure is either authorized by the individual (or someone authorized to act on the individual's behalf) or is specifically required or permitted under HIPAA. Where an individual's health information is to be used or disclosed for specific purposes other than for treatment, payment or health care operations, a written authorization is required.

¹ 45 C.F.R. Parts 160 and 164.

² Pub. L. No. 104-191.

³ Standard transactions include claims for payment.

⁴ The regulations protect individually identifiable health information, including demographic information, transmitted or maintained in any form or medium, that identifies or can be used to identify the individual, excluding education records and student medical records. "Health information" is broadly defined to include any information, oral or recorded, relating to the health of an individual, the health care provided to an individual, or payment for health care provided to an individual. HIPAA does not apply to health information that has been "de-identified" by removing, coding, encrypting or otherwise eliminating or concealing all individually identifiable information.

The rules also require Covered Entities to contract or enter into written arrangements with their “business associates,”⁵ to ensure their compliance with the privacy standards. Business associates are entities that perform or assist the Covered Entity to perform a function of that Covered Entity or who provide services to the Covered Entity.

Individuals are guaranteed certain rights under HIPAA, namely: the right to adequate notice of the Covered Entity’s privacy practices; access to their health information; amendment of their health information; accounting of disclosures; restrictions of uses and disclosures; and restrictions communicating their health information.

II. Are ISPA Members Affected By HIPAA?

Compliance with HIPAA is an achievable and required goal. If a health care provider meets the definition of a Covered Entity, it must take steps to comply with HIPAA. Since the compliance date of April 14, 2003, has passed, Covered Entities must take the steps necessary to be compliant immediately. Given that, the analysis for ISPA members begins with answering the following question: Are you/your company a covered health care provider and therefore a Covered Entity governed by HIPAA?⁶

HIPAA defines a health care provider as a provider of medical or health services and any other person or organization that furnishes, bills or is paid for “health care”⁷ in the normal course of business. For ease of determining whether an ISPA member is a covered health care provider, follow the HIPAA “Decision Tree” below:

- A. If you/your company does not furnish, bill or receive payment for health care in the normal course of business, then STOP: you/your company is not a covered health care provider.
- B. If you or your company does furnish, bill or receives payment for health care in the normal course of business, then the next question you must ask is: do you or your company conduct “covered transactions”⁸?

⁵ Business associates, such as claims processors, quality assurance and utilization review consultants, and benefit managers, to name a few, are restricted from using or disclosing PHI for any purposes other than those that are explicitly detailed in their contracts with Covered Entities.

⁶ ISPA members clearly are neither health plans nor health clearinghouses. Importantly, however, they may be considered health care providers and, as such, Covered Entities.

⁷ “Health care” means: care, services or supplies related to the health of an individual, including but not limited to: preventive, diagnostic, rehabilitative, maintenance or palliative care and counseling, service, assessment or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body, and sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

⁸ “Covered transactions” include the following: transmitting health care claims to request and obtain payment; transmitting encounter information for the purpose of recording health care;

1. If not, then STOP: you/your company is not a covered health care provider.
2. If you/your company does conduct covered transactions, then the next question you must ask is: are any of the covered transactions transmitted in “electronic form”⁹?
 - a. If not, then STOP: you/your company is not a covered health care provider.
 - b. If the covered transactions are transmitted in electronic form, then you/your company is a covered health care provider and is required to comply with HIPAA.

III. What Are The Obligations Under HIPAA Of ISPA Members Who Are “Covered Health Care Providers”?

The HIPAA privacy rules apply to individually identifiable health information maintained by Covered Entities. Individually identifiable health information includes: information related to the past, present or future physical or mental health of an individual; past, present or future payment for health services; specific care that individual has received, is receiving or will receive; information that identifies the individual receiving the care; and information someone could reasonably use to identify the individual receiving the care.

HIPAA requires a covered health care provider to take certain steps to secure the protected health information (“PHI”) of its clients/patients. PHI is a subset of individually identifiable health information. These steps include:

- ◆ Designating an individual to be the HIPAA Privacy Officer who will be responsible for complying with the privacy regulations;
- ◆ Training everyone in the work force on HIPAA, including the policy and procedures on privacy;
- ◆ Providing each client/patient with a copy of the “Notice of Uses and Disclosures,” which includes information

referral certification and authorization for health care; transmitting a health care claim status inquiry or response.

⁹ “Electronic form” means: using electronic media, electronic storage media (hard drives, magnetic tape, disks, memory cards) or transmission media used to exchange information already in electronic storage media (internet, extranet. Certain transactions, including of paper, via facsimile, and of voice via telephone, are NOT considered to be transmissions via electronic media.

related to how the covered health care provider will use the PHI; and

- ◆ Developing, adopting and implementing policies and procedures that ensure clients/patients are afforded the rights given to them under HIPAA, and that their PHI is not disclosed in violation of HIPAA.

If an ISPA member decides the company is a covered health care provider and it does not yet comply with HIPAA, it should immediately designate an individual to be the Privacy Officer. The Privacy Officer will be responsible for complying with the privacy regulations,¹⁰ and Officer should become familiar with HIPAA and any state privacy regulations affecting the company. The Privacy Officer will be responsible for helping the company develop, adopt and implement policies and procedures to help ensure that clients/patients are afforded the rights given to them under HIPAA, and that their PHI is not used or disclosed in violation of HIPAA.

Under HIPAA, individuals are given the following rights:

- ◆ Receive written notice of the privacy practices;
- ◆ Access his/her PHI;
- ◆ Request an accounting of disclosures of PHI;
- ◆ Request correction and amendment of his/her PHI;
- ◆ Request additional restrictions on the use of his/her PHI by the company; and
- ◆ Request confidential communication of PHI.

ISPA members that are covered health care providers will need policies and procedures addressing all of these rights. HIPAA specifically describes what must be included in the privacy notice and written authorizations. Once the company's policies and procedures are in place, the covered health care provider's work force must be trained on HIPAA as well as the privacy policies and procedures.

HIPAA enforcement is the responsibility of the U.S. Department of Health and Human Services ("HHS"). Initially, the enforcement process will be complaint-driven. An individual cannot sue a covered health care provider for a HIPAA violation; instead, the individual can file a complaint with HHS, which will investigate the alleged violation. HHS has the authority to impose the following penalties for HIPAA violations:

¹⁰ There also are security and transaction code set standards to comply with under HIPAA for covered health care providers.

- ◆ Civil monetary penalties of up to \$100 per violation, not to exceed \$25,000 per person for violations of a single standard in any calendar year;
- ◆ Criminal penalties of up to \$50,000 and/or imprisonment of up to five years for any person who violates such standards under false pretenses; and
- ◆ Criminal penalties of up to \$250,000 and/or imprisonment of up to 10 years for any person, who violates any standard with the intent to sell, transfer or use protected information for commercial advantage.

HHS intends to encourage and promote voluntary compliance with HIPAA's many provisions. One mechanism by which HHS seeks to accomplish voluntary compliance is by providing guidance and materials to assist Covered Entities in the implementation of HIPAA requirements.¹¹ While enforcement activities focus on obtaining voluntary compliance, the process, as noted above, is primarily complaint driven and includes progressive steps to provide opportunities to demonstrate compliance or submit corrective action plans.

Finally, if you/your company are not covered health care providers under the federal HIPAA requirements, please also be sure to check your state privacy laws and regulations to review what is required. As well, it is most wise for your company to develop a statement of privacy or confidentiality in any event, irrespective of whether HIPAA affects its operations.

Further information for interested members should be obtained through legal counsel.

¹¹ The HHS Office of Civil Rights ("OCR"), which works to promote and ensure equal access to HHS programs and services in order to further health and well-being, has many materials available on its website at <http://www.hhs.gov/ocr/hipaa> and additional technical assistance is available through the Centers for Medicare and Medicaid Services ("CMS") at <http://www.cms.gov/hipaa>.