ARIZONA ASSOCIATION
OF
HEALTH CARE LAWYERS

REPORT OF AD HOC COMMITTEE ON STANDARDS FOR ATTORNEYS AS BUSINESS ASSOCIATES UNDER HIPAA

December 1, 2004

TABLE OF CONTENTS

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[1] imposes substantial requirements on health care providers, health plans, and health care clearinghouses (otherwise known as "Covered Entities") in order to protect the privacy of patients' health information. The privacy standards of HIPAA have been implemented through regulations finalized in 2002, which, for the most part, took effect on April 14, 2003 (the "Privacy Standards").[2] One significant requirement is for Covered Entities to enter into Business Associate agreements with certain third parties to whom they disclose protected health information ("PHI").[3] These third parties are referred to as "Business Associates."[4]

Many lawyers who represent health care clients that are Covered Entities under HIPAA, including health care providers, health plans, health insurance companies, and health care clearinghouses, are considered Business Associates of the Covered Entities. Lawyers who obtain identifiable information about the client's patients or members, such as malpractice defense, transactional, or employee benefits attorneys, in order to represent the client are Business Associates.[5] In-house counsel also deal with PHI, but because they are typically employees of the Covered Entity they represent, they would not be considered Business Associates; instead, they would be subject to the requirements applicable to Covered Entities themselves.

The HIPAA Privacy Standards impact the relationships between attorneys and their clients in many ways, and the scope of that impact is still being determined, even now after most Covered Entities and their attorneys have entered into Business Associate agreements. The Arizona Association of Health Care Lawyers, as the organization representing health care attorneys in the State of Arizona, is in a unique position to provide guidance to attorneys throughout the State with respect to their obligations and expected practices when complying with the Business Associate requirements under HIPAA. The AAHCL formed an ad hoc AAHCL committee to review and analyze the issues surrounding a lawyer's responsibilities in complying with Business Associate agreements, and this document represents the final report of that committee.

This report has been approved and adopted by the AAHCL Board of Directors and constitutes AAHCL recommended practices in this area. The analysis and recommendations in this report, as well as the form documents that are included, are intended as a guide to lawyers practicing in the State of Arizona and are not intended to establish standards of care or to suggest the sole manner of dealing with the issues presented herein. Nevertheless, it is our hope that attorneys throughout the State use this report to guide their actions when dealing with HIPAA as Business

---

[1] Pub. L. No. 104-191 (Aug. 21, 1996), 42 U.S.C. § 201, *et seq.*

[2] *See* 65 Fed. Reg. 82462 (Dec. 28, 2000), *proposed modifications at* 67 Fed. Reg. 14,776 (March 27, 2002), *final modifications at* 67 Fed. Reg. 53,182 (Aug. 14, 2002), *codified at* 45 C.F.R. § 164 Part 160 and Part 164, Subpart E.

[3] PHI is defined in the Privacy Standards. *See* Section II(D), *infra.*

[4] Business Associates are specifically defined in the Privacy Standards. *See* Section II(E), *infra.*

[5] Plaintiffs' personal injury attorneys receive health information directly from their own clients, the patients, rather than from the Covered Entity, so they typically are not considered to be Business Associates of the Covered Entity. Obtaining PHI from a Covered Entity pursuant to a subpoena also does not make a lawyer a Business Associate. *See* Section VIII(F), *infra.*

Associates, so that attorneys and clients alike can achieve uniformity in their expectations of attorney conduct in these matters.

The Committee consisted of 12 dedicated attorneys who devoted a substantial number of hours in preparing this report. The members of the Committee reflected the diversity of practice areas in Arizona and came from throughout the State. The Committee included lawyers in private firms of all sizes, in-house counsel, government attorneys, and law students. Our thanks go to Daniel Benchoff, Gregory Cohen, Paul Giancola, Gordon Goodnow, Anne Kleindienst, Carla Kot, Laura Meyer, Michelle Notrica, Kristen Rosati, Susan Watchman, Linda Weaver, and Steve Goldstein, who chaired the Committee.

II. A SUMMARY OF HIPAA

A. THE HIPAA STATUTE

In 1996, Congress passed the HIPAA statute, which included the "Administrative Simplification" provisions.[6] The primary purpose of Administrative Simplification was to create national standards to facilitate the electronic exchange of health information to make financial and administrative transactions more efficient in the health care industry. Recognizing that the electronic exchange of health information in these transactions would render health information more vulnerable to confidentiality breaches, Congress also required the Department of Health and Human Services ("DHHS") to develop national privacy and security regulations.

B. THE HIPAA REGULATIONS

DHHS first published regulations to implement the national standards for administrative and financial health care transactions, called the "Standard Transactions."[7] These regulations set forth standard formats and standard data content for administrative and financial health care transactions, including health claims and equivalent health encounter information, health plan enrollments and disenrollments, health plan eligibility, health care payment and remittance advice, health plan premium payments, health claim status, referral certification and authorization, and coordination of benefits.

DHHS also published regulations to govern the privacy of health information, called the "Privacy Standards."[8] Compliance with regulations required most health care providers and health insurance companies to make substantial changes in their internal operations, their dealings with patients, and their interactions with other businesses. In summary, the Privacy Standards:

---

[6] Pub. L. No. 104-191 (Aug. 21, 1996), *amending* 1171-1179 of the Social Security Act, *codified* at 42 U.S.C. § 1320d-2 *et seq.*

[7] *See* 65 Fed. Reg. 50,312 (Aug. 17, 2000), *codified at* 45 C.F.R. §§ 160, 162, *as amended by* Fed. Reg. 38,050 (May 31, 2002). Further regulations are anticipated for additional standard transactions, including claims attachments and first report of injury. DHHS also is publishing "national identifier" regulations, which assign an identification number to participants in the health care system to make the electronic exchange of financial and administrative transactions uniform.

[8] *See* Section I, *supra.*

- Comprehensively regulate the internal use and external disclosure of PHI, creating complicated rules regarding when patient consent or authorization is required for use and disclosure, and what that consent or authorization must contain;

- Create individual patient rights to inspect and copy their own PHI, to amend erroneous or incomplete information, to obtain an "accounting" of disclosures of their information, to request a restriction of a use or disclosure for treatment, payment, or health care operations, to receive confidential communications, to receive notice of an institution's privacy practices, and to file written complaints;

- Establish a number of administrative requirements, including requiring institutions to have an extensive set of policies to protect the privacy of health information, to appoint a "privacy official" to develop those policies, and to conduct workforce training on the privacy requirements; and

- Mandate contracts with Business Associates to ensure that those associates also protect PHI.

Finally, DHHS published "Security Standards."[9] These regulations govern computer and physical security at Covered Entities. These regulations will become enforceable on April 21, 2005.[10]

The Privacy Standards are enforced by the DHHS Office of Civil Rights ("OCR"), which provides continuing guidance on interpreting the language of the regulations. The Standard Transactions and the Security Standards are enforced by the Centers for Medicare and Medicaid Services ("CMS").

C. WHAT IS A COVERED ENTITY

The Privacy Standards apply to a category of entities labeled by the rules as Covered Entities. Covered Entities are defined as:

- Health care providers that transmit certain transactions electronically;

- Health care plans (which include health care insurers and employers' group health plans); and

- Health care clearinghouses (frequently intermediaries between providers and insurers for electronic transactions, such as third party billing companies).[11]

---

[9] *See* 68 Fed. Reg. 8334 (Feb. 20, 2003), *codified at* 45 C.F.R. § 164 Part 160 and Part 164, Subpart E.

[10] *See* Section VII(A), *infra.*

[11] 45 C.F.R. §§ 160.103 and 164.104.

D. WHAT IS PROTECTED HEALTH INFORMATION

The Privacy Standards apply to a category of information labeled by the regulations as Protected Health Information ("PHI"). Generally speaking, PHI is defined as any information that:

- Is created by a Covered Entity;
- Identifies, or can be reasonably used to identify, an individual; and
- Contains information related to the past, present, or future health condition, including diagnosis and treatment, of that individual.[12]

Demographic information (including just names) is PHI if released from a Covered Entity, because it reveals that the individual received health care or is enrolled by a health insurance company.

PHI may be "de-identified." De-identified information does not identify an individual and, with respect to which, there is no reasonable basis to believe that the information can be used to identify an individual.[13] In order for information to be considered de-identified, all individual identifiers must be stripped from the information, including names; geographic subdivisions smaller than a state; dates related to the individual (except year), such as birth date or dates of service; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and license plate numbers; and device identifiers and serial numbers.[14] Once information is properly de-identified, it is no longer considered PHI.[15]

E. WHAT IS A BUSINESS ASSOCIATE

HIPAA applies directly only to Covered Entities. While DHHS was concerned about the disclosure of PHI to other entities, and the use and disclosure of PHI by those entities, DHHS had no statutory authority to regulate such entities in the Privacy Standards. As a result, DHHS created the concept of the Business Associate in order to "place restrictions on the flow of information from Covered Entities to non-covered entities."[16]

A Business Associate is any entity that:

- Performs a function or activity for, or on behalf of, a Covered Entity that involves the creation, use or disclosure of PHI. Examples include individuals or entities providing claims processing, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing services.[17]

---

[12] *Id.* at § 160.103.

[13] *Id.* at § 164.514(a).

[14] *Id.* at § 164.514(b).

[15] *Id.* at § 164.502(d).

[16] 65 Fed. Reg. 82,462, 82,504 (Dec. 28, 2000).

[17] 45 C.F.R. § 160.103(1)(i).

- Provides certain services to the Covered Entity that requires the creation, use or disclosure of PHI. Examples include entities and individuals that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.[18]

DHHS established the concept of the Business Associate in order to permit a Covered Entity to "disclose protected health information to a business associate, consistent with the other requirements of the final rule, as necessary to permit the business associate to perform functions and activities for or on behalf of the covered entity, or to provide the services specified in the business associate definition to or for the covered entity."[19]

Attorneys commented vigorously in opposition to the Notice of Proposed Rule Making in an effort to exempt attorneys representing Covered Entities from being included in the definition of Business Associates. Attorneys asserted that defining Business Associates to include attorneys would undermine the attorney/client relationship, interfere with attorney/client privilege, and was unnecessary to protect client confidences. In the preamble to the final rules, DHHS responded:

> With respect to attorneys generally, the reasons the commenters put forward to exempt attorneys from this requirement were not persuasive. The business associate requirements will not prevent attorneys from disclosing protected health information as necessary to find and prepare witnesses, nor from doing their work generally, because the business associate contract can allow disclosures for these purposes. We do not require business associate contracts to identify each disclosure to be made by the business associate; these disclosures can be identified by type or purpose. We believe covered entities and their attorneys can craft agreements that will allow for uses and disclosures of protected health information as necessary for these activities. The requirement for a business associate contract does not interfere with the attorney-client relationship, nor does it override professional judgment of business associates regarding the protected health information they need to discharge their responsibilities. We do not require covered entities to second-guess their professional business associates' reasonable requests to use or disclose protected health information in the course of the relationship.[20]

It is important to note that members of a Covered Entity's work force are specifically excluded from the definition of Business Associate. Consequently, in-house counsel and legal department staff are not Business Associates of the Covered Entity.

---

[18] *Id.* at § 160.103(1)(ii).

[19] 65 Fed. Reg. 82,462, 82,504 (Dec. 28, 2000).

[20] *Id.* at 82,642.

III. MANAGING YOUR BUSINESS ASSOCIATE AGREEMENTS

A. MANAGING YOUR BUSINESS ASSOCIATE STATUS

The general consensus is that almost all lawyers who represent health care clients will be determined to be Business Associates of their health care clients.[21] There are ways, however, for attorneys to manage their status as a Business Associate.

The primary factor that will influence the determination as to whether an attorney is a Business Associate is the nature and type of information that the client discloses to the attorney during the course of the representation. If the attorney receives PHI from the client as part of the attorney's representation, then the attorney will become a Business Associate. If the attorney can avoid receiving PHI, however, the attorney may be able to avoid becoming a Business Associate and avoid the various obligations and responsibilities that come with being a Business Associate.

RECOMMENDATION: If there is a likelihood that an attorney's representation of a client will require that the attorney obtain PHI, then the attorney should execute a Business Associate agreement with the client. Attorneys first should attempt to avoid becoming a Business Associate of their clients if possible. Methods of avoiding becoming a Business Associate include:

- Determine whether your client is actually a Covered Entity. The HIPAA Privacy Standards create certain narrow exceptions to the definition of Covered Entity. For instance, a health care provider that does not transmit health information electronically in connection with a Standard Transaction may not fall within the definition of Covered Entity. Consequently, representation of that client would not create a Business Associate relationship regardless of what information is disclosed by the client to the attorney. However, a client's status as a Covered Entity may change over time. Therefore, if an attorney is relying on the client not being a Covered Entity to avoid becoming a Business Associate, the attorney should also advise the client to notify the attorney if the client becomes a Covered Entity at some later date.

- Restrict the information that is requested from a client so as to avoid receiving PHI. Attorneys should evaluate their representation of each client to determine if obtaining PHI will be necessary in order to represent that client. If it is not necessary to obtain PHI in order to provide appropriate representation, then the attorney should avoid requesting or receiving it.

- Advise clients to refrain from sending PHI. Attorneys who determine that obtaining PHI will be unnecessary in representing a client should advise the client at the beginning of the representation that the client should not send PHI. Further, attorneys should ask clients to notify the attorney in advance if the client intends, for whatever reason, to send PHI to the attorney at any time in the future.

- Obtain Only De-Identified Information. It may be possible for an attorney to avoid becoming a Business Associate of a client by limiting the health information provided by

[21] Timothy A. Hartin, *New Federal Privacy Rules for Health Care Providers*, WISCONSIN LAWYER, April 2002.

the client to "de-identified" information. Since de-identified information is no longer PHI, disclosure of de-identified information by a Covered Entity to an attorney does not create a Business Associate relationship. Simply removing a patient's name from PHI, however, is insufficient to de-identify the information. In order for information to be considered de-identified, all individual identifiers must be stripped from the information.[22] In addition, the Privacy Standards contain certain specific requirements regarding de-identification of PHI. We recommend that (1) attorneys not utilize de-identification of PHI to avoid becoming a Business Associate because it is extremely difficult to completely de-identify health information; and (2) if an attorney does intend to pursue de-identification as a means of avoiding becoming a Business Associate, the attorney and client should carefully review the requirements for de-identifying PHI and the client's technical capability to properly de-identify PHI.

B. MANAGING YOUR BUSINESS ASSOCIATE AGREEMENTS

Managing a law firm's Business Associate agreements is a critical component of managing the firm's contractual liability as a Business Associate. Business Associate agreements can create liability in the same manner as any other contract. Consequently, appropriate administration and management of Business Associate agreements is essential to protecting an attorney and law firm.

RECOMMENDATION: Different law firms may impose different standards and policies with regard to Business Associate agreements, depending on various factors, such as their size, governing structure, or resources. Generally, however, all attorneys and law firms should:

- Treat Business Associate agreements in the same manner as the firm's fee agreements and other agreements with the client;
- Require that Business Associate agreements be reviewed and approved by a single point-of-contact within the firm or the firm's practice area who is knowledgeable about the Business Associate contracting requirements; and
- Require that an individual with authority to execute agreements on behalf of the firm sign Business Associate agreements on the firm's behalf.

C. ATTORNEY AND STAFF TRAINING

In order to manage a law firm's Business Associate agreements, it is critical that the firm train all employees and staff, both attorneys and non-attorneys, who handle or have access to PHI. The training should cover the firm's policies and procedures governing the firm's obligations as a Business Associate pursuant to the Privacy Standards and the firm's obligations pursuant to any Business Associate agreements signed with clients who are Covered Entities.

A law firm's HIPAA education and training programs will obviously vary depending upon the size of the firm and the extent to which clients of the firm are Covered Entities. Some law firms may be satisfied with a memo to all staff discussing the issues that need to be addressed, while others

[22] 45 C.F.R. § 164.514(b).

will want to have actual educational sessions to explain policies and procedures. The HIPAA education and training programs, however, should be required for all employees and staff members, whether attorneys or non-attorneys, who handle or have access to, or may handle or have access to, PHI for clients of the firm. The HIPAA training programs should focus on policies and procedures adopted by the firm in order to comply with the firm's obligations under the Privacy Standards and under any Business Associate agreements signed with clients. The training programs should be conducted by persons with knowledge of such policies and procedures and firm obligations under the Privacy Standards and the firm's Business Associate agreements.

In addition to educating and training existing employees and staff who have access to PHI, a law firm should adopt procedures to ensure that new employees and staff members (including temporaries) receive such education and training on their arrival to the law firm. Such procedures could include the following:

- Requiring that a copy of the law firm's HIPAA policy statements or procedures be included in all new employee orientation materials, or that the procedures be explained to the new employee.

- Requiring that new employees and staff hired to work in practice groups where exposure to PHI exists or may exist receive additional HIPAA training. For example, a firm with a medical malpractice section may want to tape a training program given to existing employees that could be used whenever new employees come to the firm.

- Requiring that all employees (including temporaries) be asked to sign a confidentiality statement that includes language pertaining to HIPAA and the consequences if violated.

- Requiring all employees (including temporaries) sign a receipt of policies stating that they have read and understood orientation materials relating to HIPAA.

RECOMMENDATION: Law firms that have obligations as a Business Associate of clients that are Covered Entities should adopt procedures regarding HIPAA education and training programs for attorney and non-attorney staff members who handle or have access to, or who may handle or may have access to, PHI. Law firms should take steps to inform staff of such policies, consistent with steps taken by the law firm to advise staff of other critical legal obligations. Such steps can include incorporating policies into employment manuals, issuing firm-wide memoranda, and conducting mandatory training sessions. Training programs should be conducted by persons who are knowledgeable of the firm's obligations as a Business Associate pursuant to the Privacy Standards, the firm's obligations under Business Associate agreements signed with clients that are Covered Entities, and the policies and procedures adopted by the firm to ensure compliance with such obligations. In addition to training existing employees and staff members, a law firm should adopt procedures to ensure that all new employees and staff members (including temporaries) receive education and training on the firm's obligations as a Business Associate.

IV. DEALING WITH THE ETHICAL ISSUES OF BUSINESS ASSOCIATE AGREEMENTS

A. A LAWYER'S RESPONSIBILITY TO ADVISE A CLIENT TO HAVE A BUSINESS ASSOCIATE AGREEMENT

Under the HIPAA statute and the Privacy Standards, it is the Covered Entity's obligation to enter into a Business Associate agreement.[23] In fact, liability for violations of Business Associate agreements, or the failure to obtain the necessary assurances evidenced by the Business Associate agreements, rests with the Covered Entity and not with the Business Associate.[24] Consequently, there is no obligation under HIPAA for a lawyer to advise his client of the need for a Business Associate agreement.

However, the Ethical Rules governing lawyers may impose such a requirement.[25] Under the Arizona Rules of Professional Conduct, a lawyer has a duty to act in the client's best interests,[26] and, when representing a client, a lawyer must exercise independent professional judgment and render candid advice.[27] The comments to ER 2.1 explain:

> In general, a lawyer is not expected to give advice until asked by the client. However, when a lawyer knows that a client proposes a course of action that is likely to result in substantial adverse legal consequences to the client, the lawyer's duty to the client under ER 1.4 may require that the lawyer offer advice if the client's course of action is related to the representation.[28]

Consequently, when a lawyer expects to receive PHI from a client that is a Covered Entity under HIPAA, a lawyer should be expected to know that the disclosure of such information to the lawyer without a Business Associate agreement in place could result in substantial adverse legal consequences to the client.[29]

RECOMMENDATION: If representing a health care provider, a health insurance company, a group health plan that provides health care benefits, or a health care clearinghouse, a lawyer should ask if

---

[23] 45 C.F.R. § 164.502(e).

[24] *Id.* at § 164.504(e).

[25] The Arizona Rules of Professional Conduct, Rule 42 of the Supreme Court, were recently amended by the Arizona Supreme Court pursuant to Arizona Order 2003-26 (June 2003). The Order formally took effect on December 1, 2003. All references to the Ethical Rules in this report take into account the updated language and comments in the Supreme Court's Order.

[26] 17A A.R.S. Sup. Ct. Rules, Rule 42, Rules of Prof. Conduct, ER 1.4.

[27] *Id.* at ER 2.1.

[28] *Id.* at ER 2.1, comment 5; *see also* Arizona Ethics Opinion No. 97-06 (Sept. 8, 1997) (criminal defense lawyer must advise the client about the risks associated with entering into a cooperation agreement with law enforcement agencies).

[29] It is possible that the failure to have an executed Business Associate agreement may not create substantial adverse legal consequences for the Covered Entity client. Because there has been little, if any, enforcement activity in this area, it is difficult to determine what the practical legal consequences will be. Nevertheless, the penalties in the Privacy Standards for non-compliance are significant, and it would not be prudent to rely upon possible lack of enforcement or reduced penalties at the discretion of the applicable enforcement agencies.

the client has determined if it is a Covered Entity. A lawyer is not obligated to determine if the client is a Covered Entity, unless specifically retained by the client to do so. If a lawyer expects to receive, as a result of the scope of the representation, or has received PHI from a client that the lawyer knows or should know is a Covered Entity under HIPAA, the lawyer should advise the client of the HIPAA requirement to enter into a Business Associate agreement between the client and the lawyer. A lawyer should not rely upon a client's failure to request such an agreement as an informed decision by the client not to obtain such an agreement.

B. A LAWYER'S DUTY TO UPDATE BUSINESS ASSOCIATE AGREEMENTS

As with the decision to provide initial advice to a client on the need for a Business Associate agreement, neither the HIPAA statute nor the Privacy Standards address a lawyer's responsibility to advise a client if updates to an existing Business Associate agreement are necessary. Arizona Ethical Rules impose an obligation on attorneys to keep clients informed of any information that may impact the client's ability to make informed decisions regarding the client's legal rights and obligations.[30] In addition, the Ethical Rules, in defining competent representation, state that "a lawyer should keep abreast of changes in the law and its practice."[31] On the other hand, a lawyer must be authorized by a client to take specific action. A lawyer's obligations in this regard should depend on the scope of the lawyer's representation. If the lawyer engages in general representation of the client on health care matters, then the client in all likelihood looks to the lawyer to apprise it of changes in the law that could result in substantial adverse legal consequences to the client. However, if the lawyer is retained for a specific project, the lawyer is probably not expected to provide unsolicited advice or information on matters unrelated to the project.

RECOMMENDATION: For clients with whom a lawyer has a Business Associate agreement and maintains an active attorney-client relationship that entails general representation of the client on health care matters, the lawyer should advise the client of any updates or modifications to such Business Associate agreements that may be required in order to prevent substantial adverse legal consequences to the client if such updates or modifications are not made. A lawyer is not obligated to make such updates or modifications unless specifically instructed to do so by his client. A lawyer has no obligation to advise former clients of the need to update or modify existing Business Associate agreements, since the lawyer is no longer authorized to act on behalf of that client.

C. ETHICAL ISSUES IN NEGOTIATING BUSINESS ASSOCIATE AGREEMENTS WITH CLIENTS

Once again, guidance on this issue is found only in the Ethical Rules. ER 1.8(a) prohibits a lawyer from entering into a business transaction with a client unless:

> (1) the transaction and terms on which the lawyer acquires the interest are fair and reasonable to the client and are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;

---

[30] 17A A.R.S. Sup. Ct. Rules, Rule 42, Rules of Prof. Conduct, ER 1.4 and 2.1.

[31] *Id.* at ER 1.1, comment 6.