

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

	<u>Page</u>
I. INTRODUCTION	1
II. A SUMMARY OF HIPAA	2
A. The HIPAA Statute	2
B. The HIPAA Regulations	2
C. What is a Covered Entity	3
D. What is Protected Health Information.....	4
E. What is a Business Associate.....	4
III. MANAGING YOUR BUSINESS ASSOCIATE AGREEMENTS	6
A. Managing Your Business Associate Status.....	6
B. Managing Your Business Associate Agreements	7
C. Attorney And Staff Training	7
IV. DEALING WITH THE ETHICAL ISSUES OF BUSINESS ASSOCIATE AGREEMENTS	9
A. A Lawyer's Responsibility to Advise a Client to Have a Business Associate Agreement	9
B. A Lawyer's Duty to Update Business Associate Agreements.....	10
C. Ethical Issues in Negotiating Business Associate Agreements with Clients	10
D. Waiver of Attorney-Client Privilege	11
V. REQUIRED TERMS IN A BUSINESS ASSOCIATE AGREEMENT	13
A. The Contract Must Establish the Permitted And Required Uses And Disclosures for PHI	13
B. A Business Associate Must Use Appropriate Safeguards.....	14
C. A Business Associate Must Report Any Other Uses Or Disclosures to the Covered Entity.....	14
D. A Business Associate Must Ensure Its Agents And Subcontractors to Whom It Supplies PHI Comply with the Same Restrictions Applicable to the Business Associate	14
E. A Business Associate Must "Make Available" PHI in Certain Circumstances	15
F. A Business Associate Must Make Information about Its Disclosures for Purposes Other Than Treatment, Payment Or Health Care	

	<u>Page</u>
Operations, Available to the Covered Entity for Accounting to the Patient.....	16
G. A Business Associate Must Return Or Destroy All PHI at Termination of the Contract, If Feasible, And Must Keep No Copies.....	17
H. A Business Associates Must Make Its Practice, Books And Records Relating to Use And Disclosures of PHI Received from Or Created Or Received on Behalf of a Covered Entity, Available to DHHS to Investigate Compliance of the Covered Entity	18
I. The Contract Must Authorize Termination If the Business Associate Violates a Material Term	18
J. Additional Terms Required by the Security Standards.....	18
VI. OPTIONAL TERMS COMMONLY FOUND IN BUSINESS ASSOCIATE AGREEMENTS	19
A. Indemnification Provisions	19
B. Third-Party Beneficiary Provisions.....	19
C. Minimum Necessary Provisions	19
VII. ADDITIONAL ISSUES RAISED BY THE SECURITY STANDARDS.....	20
A. Brief Description of Security Standards	20
B. Compliance with Business Associate Security Obligations.....	21
C. E-Mail Issues.....	22
VIII. DISCLOSURES TO THIRD PARTIES.....	22
A. What Agreements Are Required for Expert Witnesses, Court Reporters, Mediators, Arbitrators, Investigators, Litigation Support Personnel And Copy Services	22
B. What Agreements Are Required for Subcontractors Not Expected to Handle PHI, Such as Landlords And Janitorial Services	23
C. Special Issues for Expert And Deposition Banks	24
D. Disclosure Pursuant to Patient Authorization	25
E. Disclosure in Response to Court Order.....	25
F. Disclosures in Response to Subpoenas And Discovery Requests.....	26
1. General Discussion	26
2. Disclosures in Response to Subpoena under Arizona Law and HIPAA	27
3. Disclosures in Response to Discovery Requests under Arizona Law And HIPAA	28
G. Disclosures for Health Care Operations.....	29
H. Special Issues for Administrative Proceedings	29

	<u>Page</u>
I. Special Issues for Criminal Proceedings.....	30
J. General Recommendation Regarding Disclosures to Third-Parties in Legal Proceedings.....	30
IX. CONCLUSION	31
X. INFORMATIONAL RESOURCES REGARDING HIPAA	32
APPENDIX 1 - LAW FIRM BUSINESS ASSOCIATE AGREEMENT	
APPENDIX 2 - CONFIDENTIALITY AGREEMENT FOR AGENTS AND SUBCONTRACTORS	
APPENDIX 3A - AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION	
APPENDIX 3B - AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION	

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.

(2) the client is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel on the transaction; and

(3) the client gives informed consent, in a writing signed by the client, to the essential terms of the transaction and the lawyer's role in the transaction, including whether the lawyer is representing the client in the transaction.

Under these rules, an attorney has an obligation to suggest to the client in writing of the advantages of obtaining independent counsel and to give the client the opportunity to seek such counsel. However, one could also view the Business Associate agreement as a component of the fee agreement between the client and the attorney, in that it governs the scope of representation. No independent counsel is required for a fee agreement, and ER 1.8 specifically does not apply to such an agreement.³² A Business Associate agreement is more akin to an agreement over the scope of representation by the lawyer than a separate business transaction between a lawyer and client.

RECOMMENDATION: A lawyer, before entering into a Business Associate agreement with a client, is not obligated to advise that client of the desirability of seeking independent counsel to provide advice to the client with respect to that agreement.

D. WAIVER OF ATTORNEY-CLIENT PRIVILEGE

HIPAA requires that a Business Associate agreement contain a provision that makes the Business Associate's internal practices, books, and records relating to the use and disclosure of PHI available to DHHS for purposes of determining the Covered Entity's compliance with the Privacy Standards (the "Disclosure Requirement").³³ Although DHHS stated that this requirement was not intended to interfere with the attorney-client privilege,³⁴ HIPAA does not preclude waiver of privilege or work product protections for documents produced to DHHS pursuant to the Disclosure Requirement.

Most federal courts addressing the issue hold that disclosure to a government agency of documents protected by privilege or work product immunity waives those protections.³⁵ Only the Eighth Circuit has found that disclosure of privileged material during a formal investigation constitutes a selective waiver, allowing continued assertion of privilege in subsequent litigation with

³² See *Id.* at ER 1.8, comment 1; ER 1.5(b); but see ER 1.2(c) (a limitation of the scope of representation requires the client's informed consent).

³³ 45 C.F.R. § 164.504(e)(i)(1), (2)(ii)(H).

³⁴ 67 Fed. Reg. 53,182, 53,235 (Aug. 14, 2002).

³⁵ See, e.g., *United States v. Massachusetts Institute of Technology*, 129 F.3d 681, 682 (1st Cir. 1997) (holding voluntary production of privileged documents to a potential adversary pursuant to contractual requirements waives the attorney-client privilege and work product doctrine as against another government agency). However, the waiver may be limited to only those documents produced. See *id.*; see also *In re Martin Marietta Corp.*, 856 F.2d 619 (4th Cir. 1988) (holding waiver of privilege and non-opinion work product protection for documents disclosed to Attorney General, and underlying details, but only limited waiver of opinion work product immunity); *In re Columbia/HCA Health Care Corp.*, 293 F.3d 289 (6th Cir. 2002) (finding waiver of privilege and work product protection as to private litigant for production of internal audits to DOJ during investigation); *Westinghouse Electric Corp. v. Republic of the Philippines*, 951 F.2d 1414 (3d Cir. 1991) (holding production of internal investigation to SEC, despite confidentiality agreement, waived privilege and work product immunity as to the Philippines).

other parties.³⁶ Citing the Eighth Circuit, Arizona's Court of Appeals also found a selective waiver for documents produced to the Arizona Medical Board (fka BOMEX) during an investigation.³⁷ However, this decision was based in part on Arizona's statutory requirement for such a production.³⁸ Because it can be argued that a Business Associate's production of documents to DHHS is pursuant to contract rather than statute, the Arizona decision may be distinguishable and inapplicable. Accordingly, if DHHS requests access to privileged documents pursuant to the Disclosure Requirement, it is difficult to predict whether disclosing those documents will result in a complete, selective, or limited waiver of once applicable privilege or work product protections.

Furthermore, the Disclosure Requirement implicates a lawyer's ethical duty not to reveal information relating to representation of a client, unless the client consents after consultation.³⁹ Therefore, it is advisable to discuss the potential consequences of the Disclosure Requirement with the client prior to any disclosure.⁴⁰

RECOMMENDATION: Although the government does not anticipate it will be necessary to have access to privileged material to resolve a complaint,⁴¹ a lawyer can take steps to limit the impact of any privilege waiver resulting from such a disclosure:

- Obtain the client's consent to any disclosure. Since the waiver issue does not arise until an actual disclosure occurs, the lawyer should obtain the client's informed consent prior to making such disclosure. If the client fails or refuses to consent, the lawyer may make the disclosure because it is required by law and by the Business Associate agreement.
- Only disclose documents that reflect the Covered Entity's compliance with the Privacy Standards. The Disclosure Requirement extends to the Business Associate's internal practices, books, and records relating to the use and disclosure of PHI available to DHHS for purposes of determining the Covered Entity's compliance with the Privacy Standards.⁴² In addition, the government does not have enforcement jurisdiction over Business Associates. Therefore, the HIPAA complaint investigation should be limited to the Covered Entity's compliance with the Privacy Standards, and should not include the law firm's compliance with its Business Associate contract.

³⁶ *Diversified Industries, Inc. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1978).

³⁷ *Danielson v. Superior Court*, 157 Ariz. 41, 43, 754 P.2d 1145, 1147 (Ariz. App. 1988) (holding waiver of physician-patient attorney-client privilege is similarly analyzed and concluding physician's voluntary production of own treatment records to BOMEX pursuant to an investigation did not waive privilege).

³⁸ *Id.* at 45, 1149.

³⁹ 17A A.R.S. Sup. Ct. Rules, Rule 42, Rules of Prof. Conduct, ER 1.6.

⁴⁰ The Ninth Circuit has held that merely agreeing to waive privilege, without an actual disclosure, does not waive privilege. See *Tennebaum v. Deloitte & Touche*, 77 F.3d 337 (9th Cir. 1996) (holding promise to waive privilege in settlement agreement, without disclosure, does not constitute privilege waiver). As such, it should be difficult for an adversary to successfully argue that simply signing the Business Associate agreement constitutes waiver.

⁴¹ 67 Fed. Reg. 53,182, 53,235 (Aug. 14, 2002).

⁴² 45 C.F.R. § 164.50(e)(i)(1), (2)(ii)(H).

Because most jurisdictions recognize a limited privilege waiver (that is, a waiver limited to the subject of disclosure)⁴³ disclosure of only those records that evidence the client's compliance with the Privacy Standards (e.g., the Business Associate contract, correspondence regarding the contract, communications relating to the firm's role as a Business Associate) should limit the scope of any subsequent waiver.

- If DHHS requests record access, negotiate a confidentiality agreement. Some courts have found complete waiver unless the right to assert privilege in subsequent proceedings is reserved at the time of the disclosure.⁴⁴ Therefore, obtaining a confidentiality agreement with DHHS could be helpful in resisting subsequent privilege challenges.
- Carefully draft the Disclosure Requirement to comply with HIPAA, while limiting record access to the minimally necessary information. As an example, a modification of the CMS recommended Disclosure Requirement provision follows:

Business Associate agrees to make internal practices, books, and records, specifically relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to DHHS [in a time and manner designated by DHHS], *when requested by DHHS solely for purposes of DHHS's investigation of the Covered Entity's compliance with the Privacy Rule (Subpart E). This provision is not intended in any way to waive attorney-client privilege or work product protection applicable to the information disclosed.*

V. REQUIRED TERMS IN A BUSINESS ASSOCIATE AGREEMENT

A sample Business Associate agreement containing the recommended terms is included in Appendix 1. The specific terms are discussed in more detail in the following sections.

A. THE CONTRACT MUST ESTABLISH THE PERMITTED AND REQUIRED USES AND DISCLOSURES FOR PHI

The Business Associate agreement must specify the permitted use and disclosure of PHI by the Business Associate.⁴⁵ The Business Associate agreement may itself list the permitted uses and disclosures. Alternatively, the agreement may reference an underlying agreement (such as an engagement letter) and limit the use and disclosure of PHI by the Business Associate to those services in the underlying agreement.

⁴³ *In re Martin Marietta*, 856 F.2d at 623 (finding limited waiver as to opinion work product). *Cf. Ulibarri v. Superior Court*, 184 Ariz. 382, 909 P.2d 449 (App. 1995) (finding limited waiver as to what is placed at issue).

⁴⁴ *See, e.g., Teachers Insurance & Annuity Assoc. of Am. v. Shamrock Broadcasting Co.*, 521 F. Supp. 638 (S.D.N.Y. 1981); *In re Leslie Fay Co., Inc. Securities Litigation*, 161 F.R.D. 274 (S.D.N.Y. 1995). *Cf. United States v. Billmyer*, 57 F.3d 31 (1st Cir. 1995).

⁴⁵ 45 C.F.R. § 164.504(e)(2)(ii)(A).

The agreement also may permit the Business Associate to use the PHI for its own management and administrative services and legal obligations.⁴⁶ If this provision is not in the Business Associate agreement, the Business Associate may use and disclose PHI only for the purposes of providing the legal services specified in the engagement letter or freestanding Business Associate agreement. For example, if this provision is not in the agreement, the law firm may not disclose the PHI to its legal malpractice insurer in the event of a claim related to the case.

If the agreement permits the law firm to disclose the PHI for its own management and administrative services and its legal obligations, the agreement must limit those disclosures to two circumstances: (1) when the disclosure is required by law; or (2) if the firm first enters into an agreement with the recipient of the PHI, in which the recipient provides written assurance that he or she will hold the PHI confidentially, will use or disclose the PHI only as required by law or for the purposes for which it was disclosed to the recipient, and will notify the law firm of any breaches in the confidentiality of the PHI.⁴⁷

B. A BUSINESS ASSOCIATE MUST USE APPROPRIATE SAFEGUARDS

A Business Associate must use appropriate safeguards to prevent use or disclosure of PHI, other than as provided in the contract.⁴⁸ For example, the Business Associate should have policies in place to prevent inadvertent disclosures by its staff, or unauthorized access by outside parties. Some of the obligations contemplated by this requirement overlap a similar obligation in the Security Standards.⁴⁹

C. A BUSINESS ASSOCIATE MUST REPORT ANY OTHER USES OR DISCLOSURES TO THE COVERED ENTITY

A Business Associate must report to the Covered Entity when the Business Associate becomes aware of a use or disclosure of PHI that is not permitted by the Business Associate agreement.⁵⁰ For example, if a law firm discovers that one of its staff members was talking at a party about a particular patient in an interesting medical malpractice case, the law firm is required to report this to the Covered Entity.

D. A BUSINESS ASSOCIATE MUST ENSURE ITS AGENTS AND SUBCONTRACTORS TO WHOM IT SUPPLIES PHI COMPLY WITH THE SAME RESTRICTIONS APPLICABLE TO THE BUSINESS ASSOCIATE

The agreement must require the Business Associate to "pass-through" the agreement's terms to the "agents or subcontractors" of the Business Associate.⁵¹ DHHS reads this requirement narrowly

⁴⁶ *Id.* at § 164.504(e)(4)(i).

⁴⁷ *Id.* at § 164.504(e)(4)(ii).

⁴⁸ *Id.* at § 164.504(e)(2)(ii)(B).

⁴⁹ *See* Section V(J), *infra*.

⁵⁰ *Id.* at § 164.504(e)(2)(ii)(C).

⁵¹ *Id.* at 164.504(e)(2)(ii)(D).

and requires this pass-through agreement only when the agent or subcontractor is providing the services the Business Associate contracted to perform. For example, DHHS would interpret this requirement to apply only to other lawyers or law firms subcontracted to perform the legal services in the engagement, but DHHS does not apply the requirement to expert witnesses, court reporters, or consultants to whom the law firm discloses PHI, because those third parties are not "undertaking the functions, activities, or services that the Business Associate lawyer has agreed to perform."⁵²

E. A BUSINESS ASSOCIATE MUST "MAKE AVAILABLE" PHI IN CERTAIN CIRCUMSTANCES

The Privacy Standards require that a Covered Entity must give a patient access to his/her PHI for inspection⁵³ and also permits patients to request amendment PHI held by the Covered Entity.⁵⁴ Covered Entities are required to include in their Business Associate agreements an obligation to comply with these requirements.⁵⁵ However, these rights apply only to PHI held as a "Designated Record Set," which is defined in the Privacy Standards applicable to health care providers as "[t]he medical records and billing records about individuals maintained by or for a health care provider."⁵⁶

It will be the unusual circumstance that will require lawyers to possess, let alone maintain, Designated Record Sets. Therefore, in most instances, the requirements to permit patients to have access to or amend medical records simply will not apply to the records held by the lawyer. It is important that the Business Associate agreement's obligations in this area be limited only to the extent that the lawyer has a Designated Record Set; lawyers (or any Business Associate, for that matter) should not agree to a blanket obligation to permit patients access to, or the right to amend, PHI in their possession.

RECOMMENDATION: Unless necessary, the Business Associate should not keep Designated Record Sets. If the Business Associate has a Designated Record Set, it must be made available to the Covered Entity if the Covered Entity requests it. If a patient makes a request for a Designated Record Set from a Business Associate, the request should be referred to the Covered Entity, which would then make the decision as to access to or amendment of the Designated Record Set. The Business Associate should either send the Designated Record Set to the Covered Entity or permit access to or amendment of it only upon the written instruction of the Covered Entity. Even if the Business Associate does not have a Designated Record Set, any requests for access or amendment should be referred to the Covered Entity.

⁵² 65 Fed. Reg. at 82,506 (emphasis added); *see also* Section VIII, *infra*, for further discussion of these types of disclosures.

⁵³ *Id.* at § 164.524.

⁵⁴ *Id.* at § 164.526.

⁵⁵ *Id.* at § 164.504(e)(2)(ii)(E) and (F).

⁵⁶ *Id.* at § 164.501. For health plans, a Designated Record Set consists of "[t]he enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan." *Id.* Alternatively, for any Covered Entity, a Designated Record Set can be the records "[u]sed, in whole or in part, by or for the covered entity to make decisions about individuals." *Id.*

F. A BUSINESS ASSOCIATE MUST MAKE INFORMATION ABOUT ITS DISCLOSURES FOR PURPOSES OTHER THAN TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS, AVAILABLE TO THE COVERED ENTITY FOR ACCOUNTING TO THE PATIENT

HIPAA's Privacy Standards entitle an individual to receive an accounting of certain disclosures of PHI made by a Covered Entity in the six years prior to the date on which the accounting is requested.⁵⁷ The required accounting must include for each disclosure (i) the date of the disclosure, (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of the disclosure.⁵⁸ The Covered Entity must respond to an individual's request for an accounting within 60 days after receipt of the request, which may be extended by an additional 30 days, provided that the Covered Entity, within the 60-day period, provides the individual with a written statement of the reasons for the delay and the date by which the Covered Entity will provide the accounting.⁵⁹

Certain disclosures are excepted from the accounting requirement, including disclosures to the individual, and disclosures made "[t]o carry out treatment, payment and health care operations."⁶⁰ "Health care operations" is defined to consist of a number of activities, including "conducting or arranging for ... legal services."⁶¹ Neither the Privacy Standards, the Preamble to the proposed or final rules, or existing OCR guidance documents explain specifically what is intended to be included in "legal services" for purposes of the definition of "health care operations," but it is likely that most uses or disclosures by lawyers in the scope of their representation of a Covered Entity would be included.

The Business Associate agreement must contain a provision that obligates the Business Associate to make available the information the Covered Entity client needs in order to provide an accounting of disclosures as required by the Privacy Standards.⁶²

RECOMMENDATION: Until specific guidance is received from the OCR, lawyers should account only for disclosures of PHI outside of the scope of their representation of the Covered Entity. Examples of such disclosures include unauthorized disclosures or breaches in the lawyer's security system. If an attorney receives an individual request for an accounting of disclosures, that request should be forwarded to the Covered Entity client in a timely fashion to permit the client to handle the request within the time requirements of Section 164.528(c) of the Privacy Standards, and the lawyer should provide to the Covered Entity the required information regarding any disclosures not included within the meaning of "health care operations."

⁵⁷ *Id.* at § 164.528.

⁵⁸ *Id.* at § 164.528(b).

⁵⁹ *Id.* at § 164.528(c).

⁶⁰ *Id.* at § 164.528.

⁶¹ *Id.* at § 164.501.

⁶² *Id.* at § 164.504(e)(2)(ii)(G).

G. A BUSINESS ASSOCIATE MUST RETURN OR DESTROY ALL PHI AT TERMINATION OF THE CONTRACT, IF FEASIBLE, AND MUST KEEP NO COPIES

The Privacy Standards require a Business Associate to:

[a]t termination of the contract, if feasible, return or destroy all protected health information received from or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.⁶³

For lawyers, returning client files without keeping copies could be problematic and is contrary to the typical practice of most law firms. The Privacy Standards recognize this conflict by permitting the Business Associate to refrain from such a policy if it is "not feasible."

RECOMMENDATION: If the lawyer possesses original PHI, then the lawyer should return it to the Covered Entity client at the end of the representation. In all other instances (or if original PHI is returned and the lawyer retains copies of it), the lawyer should notify the client that return or destruction is not feasible. The lawyer must specify the reasons why return or destruction is not feasible, such as being necessary to defend against potential malpractice claims or fee disputes. The Business Associate agreement signed by the lawyer may specify in advance that return or destruction is not feasible.

Upon the end of representation of a Covered Entity client, if PHI is not returned or destroyed, the lawyer must ensure that all protections, requirements and restrictions contained in its Business Associate agreement will be extended to any retained PHI. The lawyer may, to the extent necessary, use retained PHI for the proper management and administration of its business or to carry out its legal responsibilities or as required by law.

If subcontractors or agents of the lawyer have received PHI from the lawyer during the representation, the lawyer has no obligation to monitor such PHI once disclosed and has no obligation to retrieve such PHI upon the end of the representation, unless otherwise specified in the Business Associate agreement.⁶⁴

⁶³ *Id.* at § 164.504(e)(2)(ii)(I).

⁶⁴ This is implied from the absence of an express monitoring requirement in the Privacy Standards. § 164.504(e)(2)(ii)(D) requires that the Business Associate ensure that any agents or subcontractors agree to the same restrictions and conditions applicable to the Business Associate, but does not require the Business Associate to ensure compliance with that requirement. Moreover, § 164.504(e)(2)(ii)(I) requires the return or destruction of only PHI "that the business associate still maintains," which does not include any PHI in the hands of an agent or subcontractor.

H. A BUSINESS ASSOCIATES MUST MAKE ITS PRACTICE, BOOKS AND RECORDS RELATING TO USE AND DISCLOSURES OF PHI RECEIVED FROM OR CREATED OR RECEIVED ON BEHALF OF A COVERED ENTITY, AVAILABLE TO DHHS TO INVESTIGATE COMPLIANCE OF THE COVERED ENTITY

This requirement is discussed in Section IV(D).

I. THE CONTRACT MUST AUTHORIZE TERMINATION IF THE BUSINESS ASSOCIATE VIOLATES A MATERIAL TERM

The Business Associate agreement must give the Covered Entity the ability to terminate the parties' underlying agreement (or at least terminate the disclosure of PHI to the Business Associate) if the Business Associate violates a material term of the agreement.⁶⁵

J. ADDITIONAL TERMS REQUIRED BY THE SECURITY STANDARDS

The Security Standards are discussed in Section VII. For the purposes of the Business Associate agreement itself, the Security Standards require the following provisions:

The Business Associate shall:

- A. Implement physical, administrative, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI it creates, maintains, receives, or transmits on behalf of the Covered Entity;
- B. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- C. Report to the Covered Entity any security incident of which it becomes aware;
- D. Authorize termination of the contract by the Covered Entity if the Covered Entity determines that the Business Associate has violated a material term of the contract.⁶⁶

⁶⁵ *Id.* at 164.504(e)(2)(iii).

⁶⁶ *Id.* at § 164.314(a)(2)(i).

VI. OPTIONAL TERMS COMMONLY FOUND IN BUSINESS ASSOCIATE AGREEMENTS

A. INDEMNIFICATION PROVISIONS

Many Covered Entities include in their form of Business Associate agreement a provision requiring the lawyer to indemnify the Covered Entity against unauthorized use or disclosure of PHI. Such indemnities are not required by the Privacy or Security Standards. To the extent that an indemnification provision creates liability for the Business Associate over and above its liability for a breach of the Business Associate agreement, it is not appropriate for the Covered Entity to shift that risk to the Business Associate, and it should not be included. An indemnification provision limited to liability arising out of a breach of the agreement generally adds no additional exposure beyond the liability the Business Associate already faces for contract damages. Such an indemnification provision should be deleted as unnecessary.

RECOMMENDATION: A Business Associate agreement should not contain an indemnification provision.

B. THIRD-PARTY BENEFICIARY PROVISIONS

It is not yet known whether patients of the Covered Entity would have claims against a Business Associate for violations of the Business Associate agreement that damage or harm the patient. The patient is not a party to the Business Associate agreement and therefore would not have privity of contract with the Business Associate. On the other hand, damage to the patient by unauthorized use or disclosure of that patient's PHI could be considered sufficiently foreseeable to establish liability for the Business Associate. To protect against such claims, we recommend that the Business Associate agreement make clear that it establishes rights and obligations between the Covered Entity and the Business Associate only.

RECOMMENDATION: A Business Associate agreement should state that no third-party beneficiaries are intended to be created by the agreement.

C. MINIMUM NECESSARY PROVISIONS

Although Covered Entities are required to limit use and disclosure of PHI to the "minimum necessary" level required for the purpose of the use or disclosure,⁶⁷ Business Associates are not subject to this requirement under the Privacy or Security Standards. Many Covered Entities attempt to impose this standard on the Business Associate by including it in their form of Business Associate agreement. Covered Entities have a duty, however, to disclose only the minimum amount of PHI to a lawyer as necessary for the representation.

RECOMMENDATION: A Business Associate agreement should not require the Business Associate to comply with a "minimum necessary" standard.

⁶⁷ *Id.* at § 164.502(b).

VII. ADDITIONAL ISSUES RAISED BY THE SECURITY STANDARDS

A. BRIEF DESCRIPTION OF SECURITY STANDARDS

A complete summary of the Security Standards is beyond the scope of this Report, but a brief summary is in order. The final Security Standards were effective as of April 21, 2003 (60 days after publication).⁶⁸ As with the Privacy Standards, the majority of Covered Entities have 24 months to comply with the Security Standards (until April 21, 2005); small health plans have 36 months to comply (until April 21, 2006).⁶⁹

As discussed in previous sections, HIPAA defines a "Covered Entity" as a health plan, health care clearinghouse, or provider that transmits health information connected with a covered transaction in an electronic form.⁷⁰ Once a Covered Entity is within the scope of HIPAA as a result of an electronic transaction, the Privacy Standard applies to **all** PHI held by the entity whether or not in electronic form. **The Security Standards apply only to PHI in electronic format; it does not apply to non-electronic PHI.**⁷¹

"Electronic protected health information" is PHI that is maintained or transmitted by "electronic media." This definition includes storage media (hard drives, tape, disc), transmission modes (Internet, dial-up lines, private networks, and extranet, which uses the Internet to link collaborating parties).⁷² Information that was not in electronic form prior to transmission is not transmission by electronic media.⁷³

Under the definition of electronic media, facsimiles sent by paper and voice messaging are not regulated, because the information (a piece of paper or your voice) was not originally in an electronic format. However, desktop to desktop facsimile, which transfers information directly from a computer to another computer over the Internet or network is regulated. Also regulated are automated voice interactive systems or telephone systems that uses touch tones to access information from a computer.⁷⁴ In this latter case, the Security Standards would only apply to the party that holds the information in electronic format; the party speaking into the telephone or inputting touch tones is not regulated because their information is not electronic.⁷⁵

The Security Standards require Covered Entities to address three general types of security safeguards described in the rule:

⁶⁸ 68 Fed. Reg. 8334 (Feb. 20, 2003).

⁶⁹ *Id.*

⁷⁰ 42 U.S.C. § 1320d-1(a); 45 C.F.R. § 160.103.

⁷¹ 45 C.F.R. § 164.302; 68 Fed. Reg. 8335 and 8342 (Feb. 20, 2003).

⁷² 45 C.F.R. § 160.103.

⁷³ *Id.*

⁷⁴ 68 Fed. Reg. at 8342.

⁷⁵ *Id.*

administrative safeguards, including risk analysis and management, development and implementation of security related policies and procedures, training, disaster preparedness, contingency planning and contracting (Business Associate and other);⁷⁶

physical safeguards, including controls of access to facilities and workstations, workstation security, and data handling (disposal, back up, storage);⁷⁷

technical safeguards, including technical access controls (e.g., unique user identification, emergency access, logoff procedures), audit and integrity controls, and transmission security (e.g., encryption and alternatives).⁷⁸

B. COMPLIANCE WITH BUSINESS ASSOCIATE SECURITY OBLIGATIONS

Section V(J) above discussed the terms required by the Security Standards to be in a Business Associate agreement. This Section discusses in more detail how to implement those security obligations.

As Business Associates, law firms contractually obligate themselves to implement "physical, administrative, and technical safeguards" to protect electronic PHI. Lawyers have ethical and practical obligations to protect the security of their confidential client files and information, so the Security Standards should not require extensive additional policies and procedures to be adopted. Examples of issues lawyers should consider come from guidance given by OCR regarding what are "reasonable safeguards" under the Privacy Standards:

1. An employee should be allowed routine, unimpeded access to patient medical records, only where necessary for the employee to do his job.⁷⁹
2. Physical access to information should be minimized, by isolating or locking file cabinets or record areas, or providing supervision in those areas. If patient records are in areas open to the public, care should be taken to reduce the possibility that the identifying information will be seen.⁸⁰
3. Care should be taken to limit patient information left on answering machines or in messages with left others.⁸¹
4. Computers should be secured in some fashion, such as password protection, or automatic log-off.⁸²

⁷⁶ 45 C.F.R. § 164.308(a)(1)-(7) and (b)(1).

⁷⁷ *Id.* at § 164.310(a)(1), (b), (c) and (d)(1).

⁷⁸ *Id.* at § 164.312(a)(1), (b), (c)(1), (d) and (e)(1).

⁷⁹ OCR Guidance Explaining Significant Aspects of the Privacy Rule, at <http://www.hhs.gov/ocr/hipaa/privacy.html> at 12-13 (Dec. 3, 2002 and Revised April 3, 2003).

⁸⁰ *Id.* at 16, 17-19, 27.

⁸¹ *Id.* at 16.

⁸² *Id.* at 27.

5. Before sending patient information, the sender should confirm the identity of the requester in some manner, and also confirm that the information is being sent to the proper place (e.g., confirm address or fax number). Fax machines should be in secure areas.⁸³

RECOMMENDATION: The law firm should maintain documentation of the evaluation and any policies or procedures the firm has implemented to address security issues. Each law firm's responses to these challenges will vary by the size of the firm and the nature of its health care practice.

C. E-MAIL ISSUES

The clear position of DHHS that internet communications are not secure without additional safeguards is already altering the manner and degree to which many Covered Entities choose to communicate with attorneys and other Business Associates when PHI is part of the communication. Some Covered Entities have already eliminated use of e-mail for communications involving PHI, having made a decision that e-mail does not have appropriate technical safeguards for protecting PHI. Other Covered Entities have decided that the risk of inadvertent disclosure by "hacking" or otherwise are relatively minor at present when weighed against the convenience of internet communications with Business Associates, and they continue to use e-mail that includes PHI, with or without minimizing identifying information.⁸⁴

RECOMMENDATION: Unless specifically directed by the Covered Entity client, lawyers may continue to use e-mail, faxes, and other electronic means to communicate internally and with their clients regarding PHI. However, lawyers should minimize the use of identifying information in such communications. Lawyers should adopt reasonable procedures to ensure the security of e-mail and other electronic communications.

VIII. DISCLOSURES TO THIRD PARTIES

A. WHAT AGREEMENTS ARE REQUIRED FOR EXPERT WITNESSES, COURT REPORTERS, MEDIATORS, ARBITRATORS, INVESTIGATORS, LITIGATION SUPPORT PERSONNEL AND COPY SERVICES

When a private law firm signs a Business Associate agreement with a Covered Entity client, one of the required provisions of the agreement is that the law firm must ensure that its agents and subcontractors who receive PHI agree to the same restrictions and conditions that govern the firm regarding PHI.⁸⁵ Although advisable to reduce this to writing between the law firm and its agents

⁸³ *Id.* at 119.

⁸⁴ For example, some Covered Entities have eliminated use of patient names in e-mails to persons outside the organization, using only initials and another identifier such as an account number or identification number. While such identification numbers are PHI, an unintended recipient would have to be able to access the record system of the Covered Entity in order to translate the number.

⁸⁵ 45 C.F.R. § 164.504(e)(2)(ii)(D).

and subcontractors, written agreement is not actually required in most cases. In fact, the Privacy Standards do not specifically define who constitutes an "agent or subcontractor."

The OCR narrowly construes the duty of the Business Associate to have a written agreement with its agents and subcontractors. Such an agreement is required only when the agent or subcontractor is providing the service that the law firm originally contracted to perform. An example of this is a law firm that is retained to provide legal services to a Covered Entity client and then contracts with another law firm to provide these services for the client.⁸⁶

According to the Preamble accompanying the Privacy Standards, expert witnesses are not agents,⁸⁷ and court reporters, mediators, arbitrators, litigation support personnel, investigators and copy services are probably not considered to be agents or subcontractors of private law firms. Since none of these types of individuals or companies are typically retained to perform the legal services for which the law firm is responsible, no agreement is required under HIPAA. This is not to say, however, that the parties could not enter into a confidentiality agreement in which the third person agrees to protect the information.

RECOMMENDATION: Although not required, good practice suggests that law firms acting as Business Associates should require agents and subcontractors who are given access to PHI to sign a written confidentiality agreement to adequately safeguard the protected information. A simple form of confidentiality agreement is attached as Appendix 2.

B. WHAT AGREEMENTS ARE REQUIRED FOR SUBCONTRACTORS NOT EXPECTED TO HANDLE PHI, SUCH AS LANDLORDS AND JANITORIAL SERVICES

There is no requirement for Business Associates, including law firms, to have agreements with other subcontractors that are not expected to handle PHI, such as landlords and janitorial services. These entities are not performing a service for the Covered Entity and they do not have direct access to PHI. According to the OCR:

Other Situations in Which a Business Associate Contract is NOT Required.

With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such person would be incidental, if at all.⁸⁸

RECOMMENDATION: Written confidentiality agreements are not required for landlords, janitorial services, or other similar agents or subcontractors that are not expected to handle PHI or

⁸⁶ 65 Fed. Reg. at 82,506.

⁸⁷ ". . . a covered entity has a business associate contract with a lawyer, and the lawyer discloses protected health information to an expert witness in preparation for litigation, the lawyer again would have no responsibility . . . with respect to uses or disclosures by the expert witness, because such witness is not undertaking the functions, activities or services that the business associate lawyer has agreed to perform." 65 Fed. Reg. at 82,506.

⁸⁸ *OCR Guidance, supra* note 82; see also Kristin B. Rosati and Edward F. Shay, *Your law firm signed that HIPAA business associate agreement. But is the firm complying with it?* HEALTH LAWYERS NEWS (June 2003).

who have only incidental access to PHI held by a law firm. A lawyer may rely upon internal confidentiality protections adopted by such entities relating to the conduct of their employees. A lawyer may have a written confidentiality agreement with such entities, although she is not required to do so.

C. SPECIAL ISSUES FOR EXPERT AND DEPOSITION BANKS

Law firms often maintain listings of experts and deposition banks, which consist of depositions given by experts in prior cases that involve the same issue as the lawyer's current case. Alternatively, depositions or testimony of experts in prior cases may be used in unrelated litigation for impeachment purposes. The use of such depositions, to the extent they discuss medical issues of the person involved in the prior case, could constitute a disclosure of that person's PHI by the lawyer.

When using prior expert deposition testimony, the lawyer first should analyze whether the deposition contains PHI. The lawyer is restricted as a Business Associate from using or disclosing PHI received from its Covered Entity client, so medical information in a deposition is not necessarily PHI subject to the Business Associate agreement. If the lawyer received the information from the plaintiff patient, for example, such information would not be a disclosure of PHI by a Covered Entity and subject to HIPAA. Unfortunately, it may be difficult to determine the source of the information discussed in the deposition, so determining if HIPAA is implicated can also be difficult.

Lawyers who maintain deposition or expert testimony that contain PHI must follow the HIPAA Privacy Standards in internally using and externally disclosing that PHI in subsequent lawsuits. Lawyers would be permitted to use depositions and testimony from prior unrelated cases for their own internal use, if the Business Associate agreement permits such use for administrative purposes.⁸⁹

Disclosure of that PHI in connection with subsequent litigation is a more difficult issue. Under Arizona law, the confidentiality of a plaintiff's medical records is waived by filing the lawsuit that puts his or her medical condition at issue.⁹⁰ The waiver would normally make the medical information a matter of public record and no longer privileged. However, HIPAA does not contain an express public record or waiver provision, and the OCR has not provided guidance on whether HIPAA preempts such a state waiver provision.

Where the Covered Entity client is the same in the previous and present lawsuits, PHI of any patient may be disclosed without a patient's authorization if done so by the Covered Entity for the purpose of the Covered Entity's "health care operations," which includes "conducting legal services."⁹¹ Certainly, a lawyer's internal use of such information in the course of defending a Covered Entity against a malpractice claim, for example, would be considered "conducting legal services," although there is no OCR guidance interpreting this phrase yet. Disclosure by the lawyer outside of the lawyer's office, such as introducing the prior deposition as evidence in an unrelated case, also should be considered "conducting legal services," but the greater disclosure carries greater risk because the OCR has not yet provided guidance. We thus urge caution in this area.

⁸⁹ See Section V(A), *supra*.

⁹⁰ See Section VIII(F)(3), *infra*.

⁹¹ 45 C.F.R. § 164.501(4).

