

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).

