



North Carolina Society of Healthcare Attorneys, Inc.

Report of HIPAA Security Rule Workgroup

January 31, 2005

*The information reported is general in nature, and because individual
circumstances differ, should not be construed as legal advice.*

©2005 North Carolina Society of Healthcare Attorneys, Inc.
All rights reserved

Disclaimer and User Terms:

This Report is released with the understanding that the North Carolina Society of Healthcare Attorneys, Inc. and the authors are not engaged in rendering legal advice. If you are looking for legal advice or other expert assistance, you should contact a competent professional. This Report does not create an attorney-client relationship between the authors and any other person or entity. The content in this Report may be quoted or reproduced freely provided that attribution is given to the North Carolina Society of Health Care Attorneys, Inc.

Comments?

We welcome your comments. We view this Report – like HIPAA – as a work-in-progress.

Here is contact information for our entire workgroup, but we request that you send comments to Mike Hubbard by e-mail.

Mike Hubbard
Smith, Anderson, Blount, Dorsett, Mitchell
& Jernigan, LLP
2500 Wachovia Capitol Center
Raleigh, North Carolina 27601
(919) 821-6656
mhubbard@smithlaw.com

Trish Markus
Smith Moore LLP
2800 Two Hannover Square
Raleigh, North Carolina 27601
(919) 755-8850
trish.markus@smithmoorelaw.com

Leighton Roper
Womble Carlyle Sandridge & Rice PLLC
150 Fayetteville Street Mall
Suite 2100
Raleigh, NC 27601
(919) 755-2138
lroper@wcsr.com

Bill Shenton
Poyner & Spruill, LLP
3600 Glenwood Avenue
Raleigh, North Carolina 27605
(919) 783-6400
wshenton@poynerspruill.com

McLain Wallace
Battle, Winslow, Scott & Wiley, PA
2343 Professional Drive
Rocky Mount, NC 27804
(252) 937-2200
mwallace@bwsww.com

NORTH CAROLINA SOCIETY OF HEALTHCARE ATTORNEYS, INC.

REPORT OF SECURITY RULE WORKGROUP

Table of Contents

<u>Section</u>	<u>Page</u>
1 Executive Summary.....	3
2 Introduction to HIPAA Privacy.....	8
3 Introduction to HIPAA Security.....	11
4 Other Legal Aspects of Information Security.....	14
5 Retaining Information Security Consultants	18
6 Attorney-Client Privilege	20
7 Information Security Risk Assessment.....	23
8 Information Security Management Plan.....	25
9 List of Resources	28
10 Sample Documents	30
• HIPAA Business Associate Agreement and Cover Letter	
• HIPAA Security Amendment to Business Associate Agreement and Cover Letter	

Section 1

Executive Summary

NCSHCA The North Carolina Society of Healthcare Attorneys, Inc. (“NCSHCA”) is a non-profit corporation whose mission is to provide professional education and other services to North Carolina attorneys who have an interest in health care law. NCSHCA serves as a resource to its members with a wide variety of programs and activities that reflect the diversity of health care clients. The Society holds an Annual Meeting that focuses on current and future health care legal trends and issues. It sponsors seminars throughout the year on topics of interest to its members, including federal and state legislative and regulatory developments. The Society promotes communication and networking among members.

Security Rule Workgroup NCSHCA formed this workgroup to prepare a report to help lawyers in addressing how the HIPAA Security Rule impacts law firms. This Report provides a general overview of HIPAA requirements and how these requirements directly affect clients and indirectly affect law firms.

There is evidence that the legal profession in general could do more regarding information security. An American Bar Association survey of security practices among law firms showed the following regarding their adoption of security policies:

<u>Percentage</u>	<u>Policy</u>
Computer Acceptable Use	60%
Email Use	60%
Internet Use	57%
Records Management	54%
Disaster Recovery Plan	50%

See American Bar Association, 2003 Legal Technology Resource Center Survey Report, Executive Summary, p. 7 (July 2004).

Section 1

Executive Summary, continued

Security Rule Workgroup, continued

HIPAA sets a high bar, and the Security Rule requirements, when viewed in their entirety, can seem overwhelming. The Security Rule includes “general rules” which describe what the Security Rule requires and how it works. The Security Rule also contains 22 “standards” and 42 “implementation specifications” relating to those standards. The standards are broken down into “physical,” “administrative,” and “technical” security safeguards, and these safeguards are designed to assist organizations in identifying and managing the risks posed to each organization’s information security systems and data thereon.

How HIPAA Affects Law Firms

The HIPAA privacy and security requirements affect information security for law firms in at least three key ways.

First, a law firm may be a HIPAA “business associate” of a client that is a “covered entity” under HIPAA if the firm creates or receives identifiable health information while providing legal services to a covered entity that is subject to HIPAA. In such cases, the client is required under HIPAA to sign a “business associate” agreement with the law firm that requires the law firm to safeguard the health information it creates or receives from or on behalf of the client, among other requirements.

In addition, law firms are employers. They frequently sponsor health benefits for law firm partners and employees. Health benefit plans, such as medical plans, vision plans, dental plans, and employee assistance plans can be HIPAA “covered entities” (under ERISA the benefits plans are legal entities separate and apart from the employer itself) and consequently be subject to the requirements of the Privacy and Security Rules. A discussion of employer group health plans as HIPAA covered entities is beyond the scope of this Report, and law firms’ group health plans are not further addressed in this Report. Instead, this Report focuses on how HIPAA affects law firms regarding confidential information obtained in providing legal services to clients.

Section 1

Executive Summary, continued

How HIPAA Affects Law Firms, continued

Finally, and as may become evident in the near future, some or many of the HIPAA requirements may be asserted as the standard of care or “best practices” under other legal theories for maintaining the privacy and security of confidential information. Stated differently, even if a client’s confidential information does not contain any identifiable health information, the standard of care for the law firm’s protection of the information may be asserted to be similar to the very detailed and demanding requirements under HIPAA.

What Law Firms Need To Do

If a law firm is a “business associate” of a client under HIPAA, the law firm needs to understand how HIPAA significantly affects the law firm’s responsibilities. Signing a business associate agreement is only part of the required response. The law firm needs to understand: (1) when it is appropriate for a client to share identifiable health information with the law firm; (2) what the law firm can properly do with that information; and (3) how it must protect the information.

Even when a law firm is not a HIPAA business associate, HIPAA could affect a firm’s determination about what constitutes appropriate information security measures for other types of client information that the law firm maintains. If the hospitals and medical practices in a community are required to comply with the HIPAA Security Rule’s stringent requirements to protect the privacy of their patients, then lawyers may not avoid some comparisons between this high bar set for physicians and lawyers’ duties to protect their clients’ confidential information.

Section 1

Executive Summary, continued

How this Report Helps

This report is intended to provide a high-level overview to assist lawyers in evaluating how to address their information security obligations related to HIPAA. Our goal is to highlight how HIPAA has changed the privacy landscape in the health care industry, and how such change affects the legal profession well beyond the contractual requirements of HIPAA agreements.

This report is a starting point and not the end point in analyzing how HIPAA affects law firms. To make the content more readable at a high-level overview, the authors have omitted some citations to references and have summarized at a high level various legal concepts that are detailed and subject to exceptions.

In addition to this Executive Summary, this Report contains the following sections:

Section 2: Introduction to HIPAA Privacy

Provides a broad overview of the HIPAA Privacy Rule and “business associate” agreements.

Section 3: Introduction to HIPAA Security

Provides a broad overview of the HIPAA Security Rule and “business associate” agreements related to information security.

Section 4: Other Information Security Legal Obligations

Describes examples of other legal theories that may be asserted regarding information security obligations of law firms.

Section 5: Retaining Information Security Consultants

Describes the process of considering and retaining information security consultants.

Section 6: Attorney-Client Privilege

Describes how lawyers can be of assistance to clients in encouraging frank communications under the attorney-client privilege, and also describes how law firms themselves may assert the attorney-client privilege as clients.

Section 1

Executive Summary, continued

How this Report Helps, continued

Section 7: Information Security Risk Assessment

Describes the process of performing an information security risk assessment.

Section 8: Information Security Management Plan

Describes how to use the results of the risk assessment to develop and implement an information security management plan.

Section 9: List of Resources

Provides a list of additional resources.

Section 10: Sample Documents

Describes and provides some sample documents to help illustrate the tasks and issues described in this Report.

Section 2

Introduction to HIPAA Privacy

HIPAA Statute For some time, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) has been familiar territory to employment and benefits lawyers because of the Act’s “portability” provisions related to retaining health coverage after a job change. This Report addresses Title II, Subtitle F of HIPAA, which contains the provisions on “Administrative Simplification.”

Briefly stated, HIPAA Administrative Simplification covers a variety of aspects of providing and paying for health care, including required formats and code sets for certain types of electronic transactions, national identifier numbers for providers, employers, and payors, and federal requirements relating to the privacy and security of health information that can be linked to specific individuals. Under the authority of HIPAA, the United States Department of Health and Human Services has adopted federal regulations relating to privacy and the security of individually identifiable health information. These rules are codified at 45 C.F.R. Part 160, Subparts A, B, and C, and Part 164, Subparts A and C. These regulations are called the “HIPAA Privacy Rule” and “HIPAA Security Rule” in this Report.

Adoption of Privacy Rule

The HIPAA Privacy Rule was first adopted in final form in December 2000 in the last days of President Clinton’s administration. President Bush allowed the Rule to go into effect with an initial compliance deadline of April 14, 2003. The Privacy Rule applies to “covered entities,” which are (1) health plans, (2) health care clearinghouses, and (3) those health care providers that conduct HIPAA standard transactions electronically (such as billing electronically).

Examples of health plans include insurers, HMOs, Medicare, Medicaid, and employee health benefit plans sponsored by an employer. Examples of health care providers include physicians, hospitals, pharmacies, and nursing homes.

Section 2

Introduction to HIPAA Privacy, continued

HIPAA Compliance Dates HIPAA provides for a two-year compliance period for most covered entities to comply, with an additional year for certain health plans. This two-year period begins to run on the effective date of each HIPAA rule. For example, the publication of the final Security Rule in the Federal Register in February of 2003 led to its effective date of April 21, 2003, and the initial compliance deadline is April 20, 2005.

Privacy Rule Requirements The HIPAA Privacy Rule basically defines how a covered entity may use or disclose “protected health information” (“PHI”). PHI is health information that can be linked to a specific individual. HIPAA recognizes that PHI may be found in any form of record or communication, including written and electronic formats and the spoken word and audio recordings. Even when the Privacy Rule permits a use or disclosure of PHI, additional safeguards may apply. For example, there is a general requirement to use and disclose only the “minimum necessary” amount of PHI required for the intended purpose of the use or disclosure.

Some of the Privacy Rule requirements involve a multi-step analysis to determine whether the use or disclosure may be made. It takes considerable time and energy for any organization to understand these requirements, develop compliance programs, and effectively educate and train its workforce on what is needed to comply.

The Privacy Rule provides various rights to persons who are the subject of PHI, and it also includes privacy management requirements, including the requirement to safeguard PHI from unauthorized access.

State Law HIPAA establishes a minimum level for privacy and security standards. HIPAA expressly and explicitly does not preempt State law or federal law regarding the privacy or security of PHI which may be “more stringent” than the requirements under HIPAA. In general, HIPAA views more stringent requirements as those which adopt stricter requirements for the use or disclosure of PHI or which afford individuals more rights with regard to PHI about them.

Section 2

Introduction to HIPAA Privacy, continued

Business Associate Agreements

The HIPAA Privacy Rule requires each covered entity to have a “business associate” agreement with any person or organization that receives or creates PHI while performing services on behalf of the covered entity. Lawyers who see or hear individually identifiable health information in providing legal services to a covered entity client are “business associates.” For more on law firm HIPAA business associate agreements, see the NCSHCA’s report, *HIPAA and Business Associate Agreements for Lawyers*, available at <http://www.ncshca.org/hipaabaagreement.pdf>.

With a few exceptions, the business associate agreement must prohibit a Business Associate from making any use or disclosure of PHI that the covered entity could not make. This means that when a law firm acts as a business associate, it must consider whether its covered entity client could make a use or disclosure of the PHI before the law firm itself makes the use or disclosure. The law firm has to “think like a covered entity,” even though it is not one.

Section 3

Introduction to HIPAA Security

HIPAA Security Rule

The HIPAA Security Rule was first published by the U.S. Department of Health and Human Services (“HHS”) in draft form in August 1998. It was adopted in final form in February 2003. The initial compliance deadline for the Security Rule is April 20, 2005 (April 20, 2006 for “small plans”).

The Security Rule applies to the same “covered entities” that are subject to the HIPAA Privacy Rule. Unlike the Privacy Rule, however, the Security Rule only applies to PHI that is maintained or transmitted in electronic form. Despite this difference, it may be asserted that some or many of the Security Rule standards (rightly or wrongly) are the appropriate “safeguards” required under the more broadly-worded information security requirements of the Privacy Rule and the HIPAA statute. This is, in part, because the Privacy Rule includes safeguards to protect the confidentiality, integrity, and availability of PHI.

The HIPAA Security Rule builds on the very general language about information security that Congress enacted in 1996 when it passed the HIPAA statute:

“Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—

(A) to ensure the integrity and confidentiality of the information;

(B) to protect against any reasonably anticipated—

(i) threats or hazards to the security or integrity of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) otherwise to ensure compliance with this part by the officers and employees of such person.”

18 U.S.C. § 1173(d)(2)

The remainder of this Section describes how the Security Rule provides greater detail than does the Privacy Rule regarding these general requirements.

Section 3

Introduction to HIPAA Security, continued

“General Rules” The HIPAA Security Rule contains “general” rules that describe in broad terms what covered entities must do. These rules include the following broad requirements:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI.
- (3) Protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted or required under Subpart E of this part [the Privacy Rule].
- (4) Ensure compliance with this Subpart by its workforce.

See 45 C.F.R. § 164.306(a)(1-4)

The HIPAA Privacy Rule requires each covered entity to conduct its own risk assessment with respect to scores of different aspects of information security, from physical security locks on the doors to technical security issues, like firewalls and intrusion detection. One of the unique challenges that law firms and their clients will confront in complying with the HIPAA Security Rule is the pervasive use of removable electronic media such as floppy disks, CD-ROMs, hard drives, thumb drives and other portable media. Each of these devices enhance the access to electronic information, but PHI on portable media must be accounted for by covered entities under the HIPAA Security Rule.

More Detailed “Standards” and “Implementation Specifications”

HHS has stated that in enacting HIPAA, Congress set an “exceptionally high goal” for the protection of electronic PHI (note the use of the word “ensure” in the language quoted above). The HIPAA Security Rule contains 22 broadly worded “standards” and 42 “implementation specifications” under those standards. The implementation specifications provide additional detail on what has to be done to meet the requirements of the standard. As noted above, the purpose of the implementation standards is to assist covered entities in identifying and managing physical, administrative, and technical risks to the security of the organization’s electronic PHI.

Section 3

Introduction to HIPAA Security, continued

More Detailed “Standards” and “Implementation Specifications”, continued

The 22 standards require numerous actions, including:

- conducting an accurate and thorough assessment of all reasonably anticipated threats to electronic PHI;
 - appointing a single person with oversight responsibility;
 - documenting many decisions and policies; and
 - determining whether electronic information should be encrypted.
-

Business Associate Agreements

Like the HIPAA Privacy Rule, the HIPAA Security Rule also requires that there be an agreement between a HIPAA covered entity and its “business associate.” The Security Rule requires that a covered entity must have a written agreement in which the business associate agrees to:

- implement safeguards to protect electronic PHI;
 - ensure that agents and subcontractors of the business associate agree to do the same;
 - report to the covered entity any “security incident;” and
 - authorize the termination of the agreement with the business associate if the business associate commits a material breach of the security-related provisions.
-

Sample Documents

The sample documents at Section 10 of this Report include two types of letter agreements for a “business associate” law firm to use with a client that is a HIPAA covered entity.

First, there is a sample of a letter agreement that could be a HIPAA business associate agreement that addresses *both* the HIPAA Privacy Rule and the HIPAA Security Rule.

Second, there is a sample of a HIPAA security addendum that is intended to address only the Security Rule requirements. For this document, the assumption is that there is already in place a HIPAA business associate agreement under the Privacy Rule between the law firm and the client.

Important Note: These documents are not actual agreements and are provided for illustrative and educational purposes only. Please refer to the Disclaimer and User Agreement at Page 1 of this Report.

Section 4

Other Information Security Legal Obligations

The “Non-HIPAA” World

The importance of keeping and protecting confidences is not unique to HIPAA. As this Report mentioned earlier, other legal theories may be asserted as a basis to impose information security requirements on a law firm. This section provides a brief overview of examples of other types of possible sources of information security responsibilities and obligations of law firms in that regard.

Note: This Section is only intended to highlight examples of possible sources of other obligations and is not intended to identify all types of legal theories that might be asserted relating to law firms’ and lawyers’ responsibilities for information security. It is not intended to imply that the theories discussed are applicable in any particular circumstance.

Professional Responsibility

The North Carolina State Bar has issued several advisory ethics opinions relating to a lawyer’s professional obligations to safeguard confidential client information. These include RPC 133 (July 17, 1992) regarding “Recycling Office Waste Paper,” and RPC 215 (July 21, 1995) regarding “Modern Communications Technology and the Duty of Confidentiality” (available at www.ncbar.com).

In addition to explaining responsibilities in the specific factual contexts addressed, these RPCs can be helpful when considering a law firm’s overall responsibilities for information security. Some key theories that emerge—or may be reasonably inferred—from these RPCs include:

- Some client information is more sensitive and must be protected to a greater extent than other information.
 - A lawyer has a professional obligation to protect confidential information in his or her possession from unauthorized disclosure. This professional obligation extends to the use of communications technology.
 - A lawyer has a personal and individual obligation to protect the security of client confidential information.
 - A law firm may have some information security obligations to implement internal access procedures with regard to client documents.
-

Section 4

Other Information Security Legal Obligations, continued

Professional Responsibility, continued

- The responsible attorney should take particular care to ensure that custodial personnel under his or her direct supervision understand that the attorney's professional obligations require that confidentiality of such information must be maintained.
- "A lawyer must take steps to minimize the risks that confidential information may be disclosed in a communication via a cellular or cordless telephone. First, the lawyer must use reasonable care to select a mode of communication that, in light of the exigencies of the existing circumstances, will best maintain any confidential information that might be conveyed in the communication. Second, if the lawyer knows or has reason to believe that the communication is over a telecommunication device that is susceptible to interception, the lawyer must advise the other parties to the communication of the risks of interception and the potential for confidentiality to be lost."
- "E-mail is susceptible to interception by anyone who has access to the computer network to which a lawyer 'logs-on' and such communications are rarely protected from interception by anything more than a simple password. In using e-mail, or any other technological means of communication that is not secure, the same precautions must be taken to protect client confidentiality as are set forth in opinion #1 [regarding phone calls] above."

For an article that raises a number of professional responsibility issues for lawyers regarding computer security, see Emilio Jaksetic, *Computer Security and Professional Responsibility* (June 1998), at <http://www.legalethics.com/articles.law?auth-jaks.txt> (last visited on October 4, 2004) (on file with the authors).

Contractual Duties

A client's confidentiality or non-disclosure agreement with a third party may require the client to ensure that its agents or contractors observe certain confidentiality limitations, for instance where the client receives trade secret information in the course of a joint venture with another business organization. These and other business interactions often come linked with confidentiality obligations for the client. A law firm may be asserted to be an agent or contractor of the client under such a provision.

Section 4

Other Information Security Legal Obligations, continued

Common Law Depending on the facts, there may be an assertion that a law firm has a common law duty of care to protect the security of client information.

FTC Act Under the authority of the FTC Act, the Federal Trade Commission (“FTC”) has broad regulatory authority over activities in interstate commerce that constitute unfair or deceptive commercial acts or practices. In presentations in June 2004 at a privacy conference, FTC staff suggested that inadequate security practices of a business could constitute “unfair” practices even if not deceptive (the authors are not aware that the FTC Commissioners have publicly taken this position).

Gramm-Leach-Bliley Contracts The question of whether the federal Gramm-Leach-Bliley Act (“GLB”) applies directly to law firms is beyond the scope of this Report. The authors note the decisions in *N.Y. State Bar Assoc. v. Federal Trade Commission*, No. 02-810, No. 02-1883, 2003 U.S. Dist. LEXIS 14124 (D.D.C. August 11, 2003) as well as a May 7, 2004 letter from the General Counsel of the Federal Trade Commission regarding that litigation (copy on file with the authors):

This letter represents that, unless and until the district court’s April 30, 2004 order or any judgment embodying that order is reversed, the Federal Trade Commission (FTC) will not bring any enforcement actions or conduct any investigations against practicing lawyers under Title V, Subtitle A, of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-09, for any action, inaction, or failure to comply by them during the period preceding reversal.

Section 4

Other Information Security Legal Obligations, continued

Gramm-Leach- Bliley Contracts, continued

There are other ways that GLB can affect law firm responsibilities regarding information security. For example, a client of a law firm may be regulated under GLB. If the law firm creates or receives certain types of personal information from or on behalf of the client, the client may be required under GLB to enter into an agreement with the law firm with confidentiality and security provisions.

Section 5

Retaining Information Security Consultants for Law Firms

Evaluate Need for External Expertise

One of the first decisions a law firm should make in assessing its information security risks and managing those risks is to determine the law firm's needs for external expertise in the area of information security. These needs likely will vary widely across different law firms. The decision about when external expertise may be needed should of course be based on the internal capabilities and experience of the law firm personnel regarding information security.

The "opportunity costs" to the law firm of using internal personnel also can affect the decision. For example, a law firm employee who is responsible for overseeing billing or for managing and maintaining the firm's information technology systems may have the expertise to be principally responsible for information security for the law firm. But pulling that person away from primary responsibilities may have an opportunity cost to the law firm that outweighs the hard costs of hiring an external consultant. Accordingly, the law firm should assess both its personnel and financial resources in determining whether and to what extent the firm needs external assistance with its information security duties. Also, information security is a rapidly and continually changing field, and law firm management needs to consider the time needed for internal firm personnel to keep track of and respond to developments in the field.

Issue Request for Proposals

Once the decision has been made to hire an external consultant to assist with a firm's information security program, the firm should issue a request for proposals ("RFP") for the work. The RFP can address the following factors:

- the experience and specific expertise of the consultant
 - the consultant's knowledge of the law firm's information security programs
 - the willingness of the consultant to work with and/or train the law firm's information security personnel in the appropriate processes
 - the types of remedies the consultant typically recommends
 - the consultant's deliverables
 - the cost for the consultant's services and a range of costs for compliance with the applicable information security requirements.
-

Section 5

Retaining Information Security Consultants for Law Firms, continued

Issue Request for Proposals, continued In determining which outside consultant to hire, the law firm should carefully compare the proposals received to ensure that it is getting a good price on the services it truly needs. Consultants sometimes respond to RFPs with generic statements of their services that, when translated, do not include certain key services.

Sign Contract After determining which external consultant to hire, the law firm should enter into a contract with the consultant. The contract should set forth in specific terms the consultant's duties, the amount of time the consultant is expected to be on-site, whether the consultant will train the law firm's personnel in information security techniques, what deliverables (if any) the consultant will provide, the proposed start and finish dates for the engagement, whether any follow-up duties are included, and the cost of the engagement. Including an indemnity provision is recommended, but any such clause likely will be contested or limited by the consultant.

Assess Attorney-Client Privilege A law firm may want to consider whether and to what extent the attorney-client privilege might apply to the law firm's assessment and management of its own security affairs. For example, if a law firm retains an outside lawyer to provide legal advice to the law firm relating to information security, some communications may be subject to the attorney-client privilege. Depending on the circumstances, and how the courts may view a situation, this also could include an outside law firm retaining the information security consultant on behalf of the hiring law firm.

Section 6

Attorney-Client Privilege

HIPAA and the Attorney-Client Privilege

As is often the case when attorneys counsel clients about compliance with the law, the attorney-client privilege can encourage full and frank communications between lawyer and client regarding HIPAA-related legal issues. This section briefly describes how the attorney-client privilege may be relevant to the law firm in providing legal advice to a client, *and* to the law firm when the law firm itself may be a client.

Self-Critical Analysis Privilege

Some courts have accorded a modicum of protection to an organization's internal efforts to review the quality of its goods or services. This general "self-critical analysis privilege" has received recognition in the interest of assuring that the personnel or staff of an organization "will feel free to provide the decision maker with their uninhibited opinions and recommendations....." *Skibo v. The City of New York, et al.*, 109 F.R.D. 58 (E.D.NY 1985), quoting *Coastal States Gas Corp. v. Dep't of Energy*, 199 U.S. app. D.C. 272, 617 F.2d 854, 866 (D.C. Cir. 1980).

The North Carolina courts have not recognized a general "self-critical analysis privilege" as a matter of state law. A limited privilege has been enacted by the North Carolina General Assembly for the activities of medical peer review committees. See N.C. Gen. Stat. § 131E-95(b).

Attorney-Client Privilege

Generally, the attorney-client privilege protects (i) communications (ii) between privileged persons (iii) made in confidence (iv) for the purpose of seeking legal advice. Both North Carolina courts and the Fourth Circuit interpret this privilege narrowly and strictly construe its application. The privilege also may be waived if strict attention is not paid to maintaining confidentiality of the communications.

Great care should be exercised in the application of the attorney-client privilege. It is noteworthy that the mere involvement of an attorney in reviewing a matter for a client does not guarantee that the communications that are exchanged will be deemed to be subject to the privilege. Accordingly, great care should be taken to ensure that each of the aforementioned elements of the privilege is documented before relying on the existence of its protection.

Section 6

Attorney-Client Privilege, continued

Implementation There are a variety of approaches regarding how to best maintain the attorney-client privilege in connection with an investigation of a client's compliance with the Privacy Rule or the Security Rule, as well as with respect to a law firm's evaluation of obtaining legal advice regarding its own information security obligations. The following is an example of one approach. It is not by any means intended as a template or as legal advice with respect to how the attorney-client privilege may or may not apply in a particular circumstance.

1. Before an investigation begins, XYZ management asks its counsel to undertake an investigation or supervise an investigation of the subject matter and to provide specific legal advice to management based on the investigation. This request is documented in a written request from XYZ, or in a written communication from counsel to confirm XYZ's request.
2. At the same time, XYZ management sends a memorandum directing the employees connected with the particular investigation to respond to the investigator's questions regarding the work related to the investigation and stating that the investigation is being undertaken in order to obtain legal advice for the corporation regarding its compliance with the law. This same notice should emphasize that the information exchanged is to be kept confidential. Finally, this notice also should remind the employees that the attorney conducting or supervising the investigation represents the corporation as a client, not the individual employees.
3. Legal counsel should conduct or directly supervise the investigation, so that communications made by XYZ employees to the investigator will be accorded the greatest possible protection as privileged communications.
4. Communications or reports from the investigators should be sent to legal counsel, who may in turn send them to XYZ's management.

Section 6

Attorney-Client Privilege, continued

Implementation, continued

5. The communications from investigators or counsel to management should be distributed only on a “need-to-know” basis. In addition, any dissemination to third parties outside the corporation, for example, government agencies, clients, or outside accountants, likely will waive any privilege.
 6. Any notes taken by investigators or surveys filled out by XYZ employees during the investigation should be collected and should be kept in strict confidence in order to protect the privilege attached to the underlying communications. Every document reflecting privileged communications should be stamped “Privileged and Confidential” and maintained in separate, secure files.
-

Conclusion

As noted above, the attorney-client privilege, although narrow and strictly construed, provides greater potential protection for any materials resulting from a HIPAA self-investigation process than does the self-critical analysis privilege. These steps are admittedly cumbersome, but they may be necessary to establish the privilege. It is a business decision regarding whether the benefits of the attorney-client privilege are worth the extra effort and expense.

Section 7

Information Security Risk Assessment

HIPAA Security Rule Requirements

The HIPAA Security Rule requires that a covered entity “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.” 45 C.F.R. § 164.308(a)(1)(ii)(A).

The Security Rule does not specify what level or type of risk assessment needs to be performed by a business associate of a covered entity, including a law firm acting as a business associate. However, it likely will be asserted that at least some form of risk assessment is required of a business associate in order for the business associate to meet its contractual obligation to implement safeguards that reasonably and appropriately protect electronic protected health information that the business associate receives, maintains, or transmits on behalf of the covered entity. It also stands to reason that it will be asserted that maintaining the appropriate level of security depends on a *documented* risk assessment, since such documentation assists in monitoring the effectiveness of the security compliance program.

For client information that is not protected health information under HIPAA, it similarly may be asserted that a law firm has a duty or responsibility to perform an information security risk assessment.

Assessment Process

The first step in a risk assessment is determining the law firm’s internal experience, expertise, and available resources to dedicate to the risk assessment. Section 5 contains a general discussion of whether and under what circumstances a law firm should consider retaining an outside information security consultant.

Even if external assistance will be sought, it may make sense to perform some level of internal assessment which will assist the external reviewer and help in controlling costs. This also will help a law firm become more familiar with its own information security settings and issues.

Section 7

Information Security Risk Assessment, continued

Assessment Process, continued Generally speaking, a law firm’s risk assessment itself will consist of the following elements:

- Determining where and what the firm’s information security assets are, specifically including where and what PHI is available through the information security system;
 - Determining the potential physical, administrative, and technical threats to PHI;
 - Determining which threats are most likely to occur and the costs that would accrue if those threats materialize; and
 - Evaluating these factors in a long-term perspective to determine which threats should be the firm’s primary priorities.
-

Attorney-Client Privilege

Section 6 contains a discussion of how the attorney-client privilege in the course of providing legal services can encourage open and frank communications between a lawyer and a client with respect to the course of analyzing legal compliance and risk management issues. A law firm itself also may be a client of another lawyer or law firm in this context. In addition, it is possible that in-house “general counsel” in a law firm may facilitate the protection of the attorney-client privilege over certain communications.

Section 8

Information Security Management Plan

HIPAA Requirements for Security Management

The HIPAA Security Rule requires that a covered entity “implement policies and procedures to prevent, detect, contain, and correct security violations.” The covered entity is further required to “implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [the “general rules” quoted above in this Section].” 45 C.F.R. § 164.308(a)(1)(ii)(B). Generally speaking, measures to reduce security risks should include safeguards that prevent, deter, contain, detect, and offset identified security risks. Some examples of such safeguards include firewalls, policies, insurance, modem control, data back-up and recovery, audit trails, training, a contingency plan, and encryption.

Although the HIPAA Privacy Rule does not typically apply to a law firm, the broad responsibilities for security management as described in the Security Rule could be asserted as being “best practices” that indeed are applicable to a law firm and its own information security responsibilities.

Adopt Policies and Procedures

For any compliance plan to succeed, it must have a usable and effective foundation of policies and procedures. A significant percentage of the Security Rule requirements involve documentation, through policies and procedures, of the entity’s efforts to manage the risks to information security identified through risk assessment. The challenge with HIPAA security (and information security in general) is that it is a topic that is relatively new to many people, and there are many different aspects to be addressed. It is not practical to expect an organization’s workforce to read and understand the substantial authority on information security responsibilities. The organization has to translate those responsibilities, as set by policies of the organization, to apply specifically to job responsibilities and functions within the organization.

Section 8

Information Security Management Plan, continued

Train Workforce Policies and procedures that merely sit on a shelf gathering dust do not help an organization. In fact, the fact that an organization has but ignores approved policies might be used in litigation against the organization to demonstrate that the organization did not have an *effective* compliance program. Each member of a law firm’s workforce should be trained on the information security policies and procedures that affect that person’s job responsibilities and functions, as well as on his or her approved access to confidential information.

A law firm also may sponsor a separate legal entity that is a covered entity health plan under HIPAA. In that case, the law firm will want to ensure compliance with the HIPAA Privacy Rule, and upon the compliance deadline, the HIPAA Security Rule. Training should occur for existing employees and should also be conducted with new employees. There should also be periodic reminders on security and alerts regarding new threats.

All training should be documented. As the saying goes in some HIPAA circles, “If it ain’t documented, it didn’t happen.”

Re-Evaluate

There is a common saying that “security is a process.” Almost as soon as a security management plan is adopted, it can become outdated due to new threats, the installation of new devices in the system, and other factors.

The HIPAA Security Rule requires covered entities to comply with an evaluation requirement:

Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule, and subsequently, in response to environmental or operational changes affecting the security of the electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet with the requirements of this Subpart [the Security Rule].

45 C.F.R. § 164.308(a)(8).

Section 8

Information Security Management Plan, continued

**Re-Evaluate,
continued**

It may be asserted that a law firm’s duties and responsibilities include (1) performing an initial evaluation upon completion of a risk assessment, (2) development of policies and procedures, and (3) training the law firm’s “workforce” on those policies and procedures. It may also be asserted that re-evaluation is necessary periodically thereafter to identify new threats and to manage those threats.

Section 9

List of Resources

Other Resources

The following is a short list of the many available resources regarding the topics addressed in this Report:

- Health Insurance Portability and Accountability Act of 1996, Title II, Subtitle F, Administrative Simplification, 42 U.S.C. § 1320d-1320d8.
 - HIPAA Privacy Rule and HIPAA Security Rule, 45 C.F.R. Part 160, Subparts A, B, and C, and Part 164, Subparts A and C
 - U.S. Department of Health and Human Services, (<http://aspe.os.dhhs.gov/admnsimp/index.shtml>)
 - Centers for Medicare and Medicaid Services (<http://www.cms.hhs.gov/default.asp?>)
 - Workgroup for Electronic Data Interchange (WEDI) (www.wedi.org)
 - North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) (www.nchica.org)
 - NCSHCA Privacy Rule Business Associate Report (<http://www.ncshca.org/hipaabaagreement.pdf>)
 - Rosati and Shay, *Lawyers as HIPAA Business Associates* (www.healthlawyers.org), *American Health Lawyers Association* (2004) (available for purchase)
 - Robyn A. Meinhardt, *The Role of Lawyers in HIPAA Security Compliance*, *Health Lawyers News* (Am. Health Lawyers Ass'n, Washington, D.C.), October 2004
 - *Identity Thieves Prey on Offices; 12 in Chapel Hill Hit in 2 Months*, *Raleigh News & Observer* (Raleigh, North Carolina) October 9, 2004, p. 3B
-

Section 9

List of Resources, continued

Other Resources, continued

- *Information Security Governance: Toward a Framework for Action*, Report of the Information Security Governance Task Force of the Business Software Alliance (undated c. October, 2003). Available at <http://www.bsa.org/usa/policy/Security-index.cfm>.
 - *Generally Accepted Information Security Principles*, Information Systems Security Association (Version 3.0-undated). Available at http://www.issa.org/gaisp/_pdfs/v30.pdf.
 - National Institute of Standards and Technology - <http://csrc.nist.gov/publications/index.html>
 - See for example the following NIST special publications in its 800 Series available at: <http://csrc.nist.gov/publications/nistpubs/index.html>
 - SP800-61 *Computer Security Incident Handling Guide (January 2004)*
 - SP800-50 *Building and Information Technology Security Awareness and Training Program (October 2003)*
 - SP800-48 *Wireless Network Security: 802.11, Bluetooth and Handheld Devices (November 2002)*
 - SP800-47 *Security Guide for Interconnecting Information Technology Systems (September 2002)*
 - SP800-45 *Guidelines on Electronic Mail Security (September, 2002)*
-

Section 10

Sample Documents

Disclaimer This Report contains some sample documents to help illustrate the concepts and points addressed in the Report. These documents are not intended as legal advice and should not be used as such. Please read the disclaimer on Page 1 of this Report.

HIPAA Business Associate Agreement and Cover Letter Attached as a sample document is an example of an agreement to use when a HIPAA Business Associate Agreement is not yet in place for privacy *or* security. The attached document addresses both the HIPAA Privacy Rule and HIPAA Security Rule.

HIPAA Security Rule Addendum and Cover Letter Also attached as a sample document is an Addendum to a contract or engagement letter with a client to address HIPAA Security Rule requirements. This would be used where there is already an existing business associate agreement that addresses Privacy Rule requirements.

Please note that the adequacy of legal consideration for a contract amendment should be considered when amending an existing HIPAA business associate agreement. In some cases, the amendment may be pursuant to the parties' obligations under a provision in the original business associate agreement regarding amendments of the agreement to comply with the law.

[TRANSMITTAL LETTER FOR HIPAA BUSINESS ASSOCIATE AGREEMENT]

[Law Firm Letterhead]

[Client]

Re: HIPAA Business Associate Agreement

Dear _____:

As we have discussed, the HIPAA Privacy Rule prohibits a HIPAA “covered entity” from disclosing certain individually identifiable health information to individuals and entities outside of the covered entity’s workforce who perform certain services as “business associates,” unless the business associate agrees to comply with various requirements contained in a written agreement with the covered entity.

In the course of performing legal services for you, our firm may create or receive individually identifiable health information that is “protected health information” under the HIPAA Privacy Rule. As a result, our firm may be considered a business associate, triggering the requirement for a formal Business Associate Agreement. Enclosed for your review is our firm’s standard Business Associate Agreement supplementing our prior general agreement for legal services.

The enclosed Business Associate Agreement is intended to comply with the requirements for business associate agreements under the HIPAA Privacy Rule and HIPAA Security Rule. While we would be happy to discuss the terms of the Agreement with you, we have a conflict of interest arising from the fact that we prepared, and are a party to, the Agreement. Accordingly, we advise you to seek independent counsel if you have substantive concerns about the legal ramifications of entering into the Agreement. Your execution of the Agreement will constitute your acknowledgment of the conflict, and waiver thereof to the extent of our representation of you in all related matters.

If the enclosed Agreement is acceptable, please sign as indicated and return one original to us for our files.

If you have any questions or comments, including the circumstances under which identifiable health information has been or may be disclosed to us, please contact me at (____) ____-____.

Sincerely,

[Law Firm]

Enclosure

**[HIPAA BUSINESS ASSOCIATE AGREEMENT IN FORM
OF LETTER AGREEMENT]**

[Law Firm Letterhead]

[date]

[inside address of client]

Re: HIPAA Business Associate Agreement

This letter agreement (this “Agreement”) by and among **[insert name of company or group health plan]** (the “Covered Entity”) and **[insert name of law firm]** (“Law Firm”) effective as of **[date]** (“Effective Date”). This Agreement amends and supplements any and all agreements between the parties for the provision of legal services.

Capitalized terms used in this Agreement have the meanings given them under the Health Insurance Portability and Accountability Act of 1996 and the HIPAA privacy and security regulations (45 C.F.R. Part 160, Subparts A, B, and C and Part 164, Subparts A, C and E) (the “HIPAA Privacy Rule” and the “HIPAA Security Rule”).

The Parties recognize that Law Firm is or may become a Business Associate with respect to Covered Entity to the extent it creates or receives Protected Health Information (“PHI”) from or on behalf of Covered Entity in the course of providing legal services. Accordingly, in consideration of the Parties’ ongoing relationship and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, they hereby agree as follows:

1. Contract Construction. This Agreement is intended to comply with the requirements for business associate agreements under the HIPAA Privacy Rule and HIPAA Security Rule and is to be construed to achieve compliance with those requirements.
2. Uses and Disclosures Permitted By Agreement or By Law. Law Firm may use and disclose PHI for purposes of providing legal services to Covered Entity. Law Firm will not use or further disclose PHI other than as permitted or required by this Agreement, by any agreement or engagement between the Parties for the provision of legal services, or as required by law. Law Firm will use, further disclose, and request PHI only in compliance with the “minimum necessary” provisions of the HIPAA Privacy Rule.

3. Uses and Disclosures Permitted by HIPAA. Law Firm may not use or further disclose the information in a manner that would violate the requirements of the HIPAA Privacy Rule if done by Covered Entity, except that Law Firm may use and disclose PHI for the proper management and administration of the Law Firm or to carry out its legal responsibilities consistent with the provisions of 45 C.F.R. §§ 164.504(e)(4)(i) and (ii). Law Firm may only disclose PHI for such purposes if:
 - a) the disclosure is required by law; or
 - b) Law Firm obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Law Firm of any instances of which it is aware in which the confidentiality of the information has been breached.
4. Safeguards. Law Firm will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement
5. Mitigation. Law Firm agrees to mitigate, to the extent practicable, any harmful effect that is known to Law Firm of a use or disclosure of PHI by Law Firm in violation of the requirements of this Agreement.
6. Reporting of Certain Disclosures. Law Firm will report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware.
7. Agents/Subcontractors. Law Firm will ensure that its agents, including any subcontractors, to whom it provides PHI received from, or created or received by Law Firm on behalf of, Covered Entity, agrees to the same restrictions and conditions that apply to Law Firm with respect to such information.
8. Access. Law Firm agrees to provide access to PHI at the request of Covered Entity, and in a reasonable time, manner, and place designated by Covered Entity, to Covered Entity or, as directed by Covered Entity, to an individual to enable Covered Entity to meet its obligations under 45 C.F.R. § 164.524 to provide individual access to such PHI. Law Firm's obligations under this Paragraph apply only to PHI in Designated Record Sets in Law Firm's possession or control.
9. Amendment. Law Firm will make PHI available to Covered Entity in a reasonable time, manner, and place designated by the Covered Entity, to enable Covered Entity to meet its obligations under C.F.R. § 164.526 to amend incomplete or inaccurate PHI and incorporate any amendments to PHI as Covered

Entity may instruct. Law Firm's obligations under this Paragraph apply only to PHI in Designated Record Sets in Law Firm's possession or control.

10. Accounting. Law Firm will make PHI and information related to disclosures of PHI by Law Firm available to Covered Entity in a reasonable time, manner, and place designated by the Covered Entity, to enable Covered Entity to meet its obligations under C.F.R. § 165.528 to account for uses and disclosures of PHI. Law Firm's obligations under this Paragraph apply only to those disclosures for which Covered Entity would be required to provide an accounting.
11. HHS Access. If Law Firm receives a request made on behalf of the Secretary of the Department of Health and Human Services, Law Firm will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the HIPAA Privacy Rule. Unless otherwise required by law or authorized by Covered Entity in writing, however, Law Firm will not disclose any confidential or privileged information received from, or created or received by Law Firm on behalf of, Covered Entity to the Secretary or any other third party, and this Agreement does not waive or amend either the attorney/client privilege, the attorney work product doctrine, or other privileges or protections.
12. Breach. Upon Covered Entity's knowledge of a material breach by Law Firm of this Agreement, Covered Entity shall provide an opportunity for Law Firm to cure the breach or end the violation. If Law Firm does not do so within the time specified by Covered Entity, Covered Entity may terminate this Agreement and the attorney-client relationship. If Business Associate has breached a material term of this Agreement and cure is not possible, Covered Entity may immediately terminate this Agreement and the attorney-client relationship.
13. Return or Destruction of PHI. Upon termination of this Agreement for any reason, Law Firm will return or destroy all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form and retain no copies of such information if feasible. Because of Law Firm's responsibility to maintain a record of the services it provides, return or destruction of such information will generally not be feasible. If such return or destruction is not feasible, Law Firm will extend the protections of this Agreement to the information retained and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
14. Termination. If not sooner terminated, this Agreement shall terminate when all the PHI created or received by Law Firm from or on behalf of Covered Entity is destroyed or returned to Covered Entity.

15. No Third Party Beneficiary. This Agreement is intended for the sole benefit of the Parties and does not otherwise create any third party beneficiary rights, except to the extent that the HIPAA Privacy Rule validly requires the Secretary of the Department of Health and Human Services to be a third party beneficiary to this Agreement.
16. Amendment of Terms and Conditions. This Agreement cannot be amended except by the mutual written agreement of the Parties.
17. Amendment for Compliance. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remaining provisions of this Agreement will remain in full force and effect. In addition, in the event Covered Entity believes in good faith that any provision of the Agreement fails to comply with the then-current requirements of the HIPAA Privacy Rule, Covered Entity shall so notify Law Firm in writing. For a period of up to 30 days, the parties shall address in good faith such concern and shall amend the terms of this Agreement, if necessary to bring it into compliance. If after such 30-day period this Agreement fails to comply with the HIPAA Privacy Rule with respect to the concern(s) raised pursuant to this Paragraph, then Covered Entity has the right to terminate this Agreement and the attorney-client relationship upon written notice to Law Firm.
18. Other Safeguards. Effective as of the later of April 20, 2005 or the Effective Date specified on the first page of this Agreement, Law Firm will:
 - (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of 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; and
 - (C) Report to Covered Entity any security incident of which it becomes aware, provided that the term “security incident” as used in this Agreement and as construed with respect to the term as defined in the HIPAA Security Rule is subject to guidance or clarification from the Centers for Medicare and Medicaid Services (“CMS”) with respect to a threatened incident that does not result in a security breach (for example, “pings” on a network firewall).

To acknowledge your agreement to the terms and conditions in this letter, please indicate so by signing the enclosed copy of this letter in the place provided below and returning the executed copy to my attention.

Thank you.

Sincerely,

[LAW FIRM]

By: _____

Acknowledged and Agreed:

[CLIENT]

By: _____

Title: _____

Date: _____

[TRANSMITTAL LETTER FOR SECURITY RULE AMENDMENT
TO HIPAA BUSINESS ASSOCIATE AGREEMENT]

[Law Firm Letterhead]

[Client]

Re: Amendment to HIPAA Business Associate Agreement to Address HIPAA Security Rule

Dear _____:

In the course of performing legal services for you, our firm may create or receive individually identifiable health information that is “protected health information” under the HIPAA Privacy Rule. As a result, our firm may be considered a business associate, triggering the requirement for a formal Business Associate Agreement under the HIPAA Privacy Rule. Our records reflect that our firm has a signed Business Associate Agreement with you.

As we have discussed, the HIPAA Security Rule has a compliance deadline of April 20, 2005 (April 20, 2006 for “small” health plans). Enclosed for your review is our firm’s standard Amendment to Business Associate Agreement supplementing the existing Business Associate Agreement between us and our prior general agreement for legal services to include provisions required by the HIPAA Security Rule.

The enclosed Amendment to Business Associate Agreement is intended to comply with the requirements for business associate agreements under the HIPAA Security Rule. While we would be happy to discuss the terms of the Agreement with you, we have a conflict of interest arising from the fact that we prepared, and are a party to, the Agreement. Accordingly, we advise you to seek independent counsel if you have substantive concerns about the legal ramifications of entering into the Agreement. Your execution of the Agreement will constitute your acknowledgment of the conflict, and waiver thereof to the extent of our representation of you in all related matters.

If the enclosed Agreement is acceptable, please sign as indicated and return one original to us for our files.

If you have any questions or comments, including the circumstances under which identifiable health information has been or may be disclosed to us, please contact me at (____) ____-____.

Sincerely,

[Law Firm]

Enclosure

AMENDMENT TO BUSINESS ASSOCIATE AGREEMENT

Covered Entity: [insert name of group health plan]
Business Associate: [insert name of law firm]
Business Associate Agreement: _____
Effective Date of Amendment: _____

This Amendment to Business Associate Agreement (this “Amendment”) is made by and between the “Covered Entity” named above and the “Business Associate” named above, effective as of the Effective Date specified above.

This Amendment modifies and is made a part of the Business Associate Agreement(s) between Covered Entity and Business Associate identified above. The purpose of this Amendment is to supplement the provisions of the Business Associate Agreement(s) to include provisions intended to comply with the requirements for business associate agreements under the HIPAA “Security Rule,” which has an initial compliance deadline of April 20, 2005 (April 20, 2006 for “small” health plans).

This Amendment amends the Business Associate Agreement by adding the following provisions:

Business Associate agrees to:

- (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of 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; and
- (C) Report to Covered Entity any security incident of which it becomes aware, provided that the term “security incident” as used in this Agreement and as defined in the HIPAA Security Rule is subject to guidance or clarification from the Centers for Medicare and Medicaid Services (“CMS”) with respect to a threatened incident that does not result in a security breach (for example, “pings” on a network firewall).

All other aspects of the Business Associate Agreement remain unchanged.

BUSINESS ASSOCIATE

By: _____

Its: _____

Date: _____

COVERED ENTITY

By: _____

Its: _____

Date: _____