HIPAA FOR LAWYERS AND LAW FIRMS

What you need to know to prevent your law firm from paying MILLION$

FDCC Annual Meeting
The Greenbrier Resort
White Sulphur Springs, West Virginia
July 27 – August 2, 2014

Presented by:

James A. Hoover
Burr & Forman, LLP
Birmingham, Alabama
jhoover@burr.com

Robert L. Coffield
Flaherty Sensabaugh Bonasso PLLC
Charleston, West Virginia
RCoffield@fsblaw.com

Robert L. Coffield is a health care attorney and partner at Flaherty Sensabaugh Bonasso PLLC in Charleston, West Virginia. Mr. Coffield helps and provides legal advice to a variety of business and health care clients. His clients include hospitals, physicians, long term care facilities, home health providers, and health technology companies.

Mr. Coffield represents clients involved in regulatory litigation, certificate of need, professional licensure matters, and business transactions. Mr. Coffield advises clients on regulatory compliance issues, privacy, security, HIPAA/HITECH compliance, and other state/federal health law issues. He is involved in and an expert on the legal impact of health care social media, health 2.0, and other technology on our health care system.

Mr. Coffield serves on the Board of the West Virginia Health Information Network, West Virginia's HIE, and is involved in various other health information related projects on the state and federal level. Mr. Coffield is a member of the American Health Lawyers Association and serves as the Vice Chair of Publications for the Health Information Technology Practice Group. Mr. Coffield is a founding Board Member of Create West Virginia. Mr. Coffield has been recognized by his peers for inclusion in Best Lawyer in America – Health Care category since 2008.

Mr. Coffield graduated from Bethany College in 1988 with a BA, English and obtained his JD from the West Virginia University College of Law in 1993. Mr. Coffield was the author of Health Care Law Blog from 2004 through 2012, and now provides social media commentary on health care and technology related law industry news via Twitter at @BobCoffield.

James A. Hoover practices in the Burr & Forman LLP Health Care Practice Group. Jim represents numerous hospitals, physician practices, pharmacies and other healthcare providers throughout Alabama and the southeast in a variety of matters. His experience includes defending healthcare providers in a variety of government investigations led by such government agencies as the OIG, OCR, FBI, FDA, CMS, DEA and DOJ. He has handled countless matters before administrative tribunals, as well as representing healthcare providers with their compliance programs, certificate of need issues, medical staff credentialing, responding to alleged EMTALA violations, Medicare appeals, audits, recoupments and sanctions, HIPAA privacy and security matters, as well as trying their commercial litigation disputes.

Jim frequently lectures on the requirements imposed by HIPAA and implementing a HIPAA compliance program, and other health care compliance issues. He authored Chapter 9 of the Health Law Handbook, 2005 edition entitled "The Emergency Medical Treatment and Active Labor Act: Responding to an Active Investigation." Most recently, he co-authored the Alabama Association of Health Information Management's Medical Records Manual as well as numerous articles on health law related topics for publications such as the Birmingham Medical News; Inside Counsel and Pharmaceutical Compliance Monitor.

Jim has been selected for inclusion in The Best Lawyers in America (Health Law) since 2010 and Alabama Super Lawyers in the area of Health Care Law since 2011. Jim is a past-Chairman of the Alabama Bar Health Law Section and past-Chairman of the Board of Trustees of the Alabama Bar Lawyer Referral Service. He currently serves as the Secretary of the Board of Directors for Kid One Transportation, non-profit organization in the State of Alabama. Jim is a member of the American Bar Association, the Alabama State Bar, the Birmingham Bar Association and the American Health Lawyers Association. He is a Martindale-Hubbell AV rated attorney and a former recipient of the Birmingham Business Journal's "Top 40 Under 40" honor.

Jim received his B.B.A. in Risk Management and Insurance in 1987 from the University of Georgia and his J.D. in 1992 from Cumberland School of Law at Samford University.

I. Introduction

For years now lawyers and law firms providing professional services to health care providers or health insurance plans should have had in place essential safeguards to meet the responsibilities and requirements as business associates under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA and the related privacy and security rules governing how health care providers, health insurance plans and others (defined under HIPAA as "covered entities") are allowed to use and disclose health and medical information (defined under HIPAA as "protected health information") have been in effect since 2003. However, many third parties, including lawyers and law firms, who regularly handle health information on behalf of their client covered entities while providing professional services have not taken seriously their duty and responsibility to safeguard such information in full compliance with HIPAA and its associated regulations.

On January 17, 2013, the Office of Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") issued the long awaited final rule ("Final Rule") amending the HIPAA privacy, security, enforcement and breach notification rules in accordance with the Health Information Technology for Economic and Clinical Health ("HITECH"),[1] which significantly expands certain obligations for health care providers and their business associates. The Final Rule, published in the Federal Register on January 25, 2013, has been described as "the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented."

With the issuance of the Final Rule in accordance with HITECH lawyers and law firms must take compliance efforts seriously or face significant legal and regulatory risk from clients and government agencies tasked with enforcing HIPAA. Under the most recent Final Rule revisions to HIPAA the responsibilities of business associates have increased and the penalty structure for violating the regulations have radically increased. The Final Rule revisions increased enforcement and mandated auditing by the OCR increasing the chances of lawyers and law firms being subjected to liability associated with breaches of privacy or security of client sensitive health information, violation of the regulations or random auditing by OCR and its contracted auditors.

In general, the Final Rule expands HIPAA obligations for business associates and their subcontractors, revises the requirements regarding the use and disclosure of patient information, expands patient rights, clarifies the content of the Notice of Privacy Practices to be provided by healthcare providers, modifies the breach notification requirements, and expands enforcement provisions and penalties. The Final Rule became effective March 26, 2013. However, health care providers and business associates had until September 23, 2013 (and in limited circumstances with respect to amending business associate agreements, until September 23, 2014) to achieve compliance with many of the new provisions.

[1] See Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under the HITECH Final Omnibus Rule, 78 Fed. Reg. 5566 (January 25, 2013) ("Final Rule" sometimes referred to as the "Omnibus Rule").

A copy of the Final Rule can be obtained and downloaded at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

II. Is My Law Firm A HIPAA Business Associate?

Lawyers and law firms who obtain or access protected health information from a health care provider or health insurance company or other covered entity under HIPAA when providing professional legal services to that client, or to a business associate or subcontractor of that client, are designated as business associates under HIPAA. As a business associate the lawyer or law firm is required to use and disclose that client's protected health information only in accordance with the terms of a signed business associate agreement (commonly referred to as a "BAA") outlining the HIPAA requirements, restrictions on use and disclosure of the information obtained from the client, obligations when sharing the information with other third parties and compliance requirements. Lawyers and law firms need to develop and implement written HIPAA policies and procedures addressing the HIPAA requirements as a business associate, educate and train workforce members and regularly monitor compliance effort.

Compliance Obligations

The Final Rule clarifies that business associates and their subcontractors are now directly liable under HIPAA, must comply with the HIPAA Security Rules and are responsible for limiting uses and disclosures of protected health information ("PHI") as set forth in their business associate agreement and as required by the HIPAA Privacy Rule. Under the Final Rule business associate are now directly liable for impermissible uses and disclosures of PHI. The business associate is also directly liable for failing to provide breach notification to a covered entity when unsecured PHI is lost or inappropriately accessed, used or disclosed. In addition, business associates under the Final Rule are liable for failing to provide access to a copy of the electronic PHI to the covered entity, the individual whose PHI is held by the business associate or the individual's designee or provide an accounting of disclosures of PHI. Further, a business associate can now be held directly liable for failing to disclose PHI to the Secretary of the Centers for Medicare and Medicaid Services related to an investigation by the Secretary on whether the business associate is compliant with HIPAA. Last, business associates and their subcontractors are directly liable for failing to comply with the requirements of the HIPAA Security Rule.

However, not all HIPAA Privacy Rule requirements apply to business associates and their subcontractors. For example, business associates do not need a Notice of Privacy Practices and do not need to designate a privacy officer. However, business associates and their subcontractors are now directly liable for violations of their HIPAA obligations. Further, business associates are liable for failing to enter into a subcontractor business associate agreement with a subcontractor that creates or receives PHI for the covered entity.

The Final Rule grandfathers current business associate agreements for up to one year, until September 23, 2014, if the agreements were in place prior to January 25, 2013, were fully HIPAA compliant and are not renewed or modified during the one year grandfather period. If a

business associate agreement was not compliant as of January 25, 2013, is renewed or modified during the grandfathered period or if a subcontractor agreement with a business associate was not in place, then the compliance date for updating or entering into compliant agreements is September 23, 2013.

Expanded Definition

Under HIPAA, a covered entity (*e.g.*, healthcare providers, health plans and health care clearinghouses) can disclose PHI to a business associate, which is generally a person or entity that performs functions, activities or services on behalf of the covered entity that involve the use and/or disclosure of PHI. For a covered entity to use the services of a business associate, the covered entity must enter into a business associate agreement with the business associate. The business associate agreement obligates the business associate to comply with the HIPAA Security Rule and certain HIPAA Privacy Rule provisions.

For lawyers and law firms the critical question is whether the client relationship they have is one that obligates them and classifies them within the definition as a business associate. If the lawyer or law firm provides professional legal services to a covered entity where the provision of the service involves the disclosure of PHI (e.g., medical or health records, billing records, etc.) to the lawyer then the lawyer or law firm is a business associate under HIPAA. For example, if the firm represents a hospital, physician or other health care provider and needs to obtain from the client PHI to represent the client, such as a professional liability claim, then a business associate relationship exists and the law firm is required to comply with HIPAA, regardless of whether the law firm signed a business associate agreement.

The Final Rule clarified and named three specific types of entities as falling under the "business associate" definition, including entities that transmit and routinely access PHI on behalf of a covered entity (patient safety organizations, health information organizations, e-prescribing gateways, etc.), personal health vendors acting as covered entities, and business associate subcontractors. For lawyers and law firms the most challenging of the three is the extension of HIPAA to subcontractors. Lawyers and law firms who obtain or maintain PHI on behalf of their business associate clients are required to comply with all applicable HIPAA provisions, despite the fact that the client is not an actual "covered entity" under HIPAA. In the role of representing a business associate under HIPAA the lawyer or law firm is required to enter into a Subcontractor Business Associate Agreement. The expanded definition of business associate under the Final Rule causes potential downstream regulatory liability for business associate provisions that it may not even be aware of or contractually liable for. Thus, lawyers and law firms need to closely assess its clients when PHI is provided to them to determine whether there may be some upstream responsibility to covered entities that contract with the client. Further, by expanding the definition of business associate to a person or entity that creates, receives, *maintains*, or transmits PHI on behalf of a covered entity, data storage providers, even if they do not access a covered entity's PHI, are now considered business associates. However, an entity that is merely a conduit of PHI and does not require access (such as the U.S. Post Office or an internet service provider (ISP)) is not considered a business associate.

Subcontractors

As mentioned above, the Final Rule includes subcontractors in the definition of business associates. A "subcontractor" is defined as a person or entity to which a business associate delegates a function, activity, or service. Accordingly, a subcontractor of a business associate that creates, receives, maintains or transmits PHI on behalf of the covered entity is now considered a business associate and must comply with HIPAA to the same extent as the business associate. For example, if a covered entity hires a business associate to handle PHI document and media shredding and the business associate retains a subcontractor to help with that service, then the subcontractor would be required to comply with the requirements of the HIPAA Security Rules (*e.g.*, with respect to the proper disposal of electronic PHI) and the HIPAA Privacy Rules (*e.g.*, with respect to limiting its uses and disclosures of PHI in accordance with its contract with the business associate.) It is the business associate's obligation, not the obligation of the covered entity, to make sure that a proper subcontractor business associate agreement is in place between the business associate and the subcontractor. Business associates and their subcontractors are directly liable for violations of their HIPAA obligations.

In the context of law firm compliance, this means that law firms need to develop internal procedures that recognize those third party business arrangements that trigger the requirement to put in place a subcontractor agreement. For example, law firms often subcontract for expert witnesses, copy and technology companies, e-discovery services, forensic computer experts and other types of staffing organizations. If these subcontracts regularly handle PHI then the subcontractors must meet the same business associate requirements that are applicable to the law firm. The law firm has a duty and responsibility to its client and is likely contractually required under the business associate agreement to advise and oversee these subcontractors use of PHI and assess the awareness of the subcontractor's regulatory awareness of HIPAA.

III. Security Rule Requirements

The HIPAA Security Rule applies only to electronic PHI ("ePHI") and highlights various requirements on the administrative and technical safeguards required to protect such ePHI. Under the Security Rule there are "required" and "addressable" implementation specifications. The Security Rule takes a very practical approach to compliance – recognizing that business associates come in all sizes. For example, a solo practitioner who is a business associate as compared to a large national or international law firm with thousands of lawyers. The Security Rule provides implementation flexibility by providing general compliance concepts rather than detailed security requirements.

Generally, the Security Rule requires lawyers and law firms to implement a security risk management plan that includes conducting a risk analysis to determine the type of safeguards necessary based on the scope and size of the business associate. The risk analysis included assessing potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI acquired, used or maintained by the business associate. The business associate law firm is required as a part of the Security Rule to name a person as the security official responsible for implementing and overseeing security for the business associate. The security risk management plan involves core implementation specifications to reduce the risks of a security incident,

including implementing administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of ePHI.

IV. Breach Notifications

HIPAA requires that covered entities provide notification to affected individuals and the Secretary of HHS following the discovery of a breach of unsecured PHI. In some cases, HIPAA requires covered entities to also notify the media of breaches. The term "breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information. Prior to the Final Rule, HIPAA allowed covered entity's to determine if the security or privacy of PHI was compromised based on a "harm standard". This standard provided that a breach of PHI would not have occurred unless the disclosure presented a significant risk of financial, reputational or other harm to the individual. Accordingly, a covered entity could analyze a breach of PHI and if it determined that the harm standard was not met then the disclosure of the breach was not required.

The Final Rule eliminates the "harm standard" and instead provides that an impermissible use or disclosure of PHI is presumed to be a breach and therefore notification is required unless a covered entity can demonstrate and document that there is a "low probability that the PHI has been compromised." A covered entity is required to consider and document four factors to determine whether the new "low probability" standard has been met:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

The Federal Register comments to the Final Rule provide substantial discussion of the analysis that a covered entity must undertake to determine if there is a low probability that the PHI has been compromised. It is clear from the discussion and examples provided in the Final Rule, that the Office of Civil Rights believes that it will be very difficult for a covered entity to demonstrate that a breach meets this new "low probability" standard. However, it is not clear that the new standard for determining a breach will result in a more objective analysis.

As stated above, when a breach of PHI occurs a covered entity has an obligation to report the breach to the affected individual, the Secretary of HHS and possibly the media. The obligation to report, and the time-frame for reporting, occurs once the covered entity "discovers" the breach. The Final Rule maintains the current breach notification requirements without modification, but provides clarification on when a breach is discovered, the time-frame for reporting a breach, methods of notification, and the content of the notice.

- Under HIPAA a breach is discovered once an employee, officer, or other agent of the covered entity "knows or should reasonably have known of the breach." The comments to the Final Rule provide that a covered entity must excise reasonable diligence to determine a breach, and that such determination is generally a factual one, since what is reasonable depends on the circumstances. Factors to be considered include whether a covered entity took reasonable steps to learn of the breaches and whether there were indications of breaches that a person seeking to satisfy HIPAA would have investigated under similar circumstances.

- HIPAA requires covered entities to notify individuals of a breach within 60 days from the discovery of the breach, except if law enforcement requests a delay. The Final Rule makes it clear that the time period begins to run when the incident becomes known, not when it is determined that a breach as defined by HIPAA has occurred.

- The content of any breach notification is provided for in the HIPAA rules, and generally requires: (i) a brief description of the breach, (ii) a description of the type of PHI involved in the breach, (iii) any steps the individual should take to mitigate harm from the breach, and (iv) a description of what the covered entity is doing to investigate and mitigate the breach, and (v) contact procedures for the individual to ask questions or obtain more information. The Final Rule makes it clear that a notice has not been given if undeliverable, but does allow notification by email in certain circumstances. Further, if more than 10 notices are returned and the covered entity is unable to identify correct addresses or contact information within the 60 day notice period, the covered entity is required to post notices on its website.

Lawyers and law firms need to focus much of their compliance efforts under HIPAA on structuring internal controls that promote the reporting and investigating of data incidents and potential breaches of PHI. Law firms that represent health care clients and regularly deal with PHI are at a high risk for some type of data incident which may require internal investigation and possible reporting as a breach under HIPAA. This type of security incident require a very fact specific analysis to determine whether such incident rises to the level of a reportable breach under the rules. Most business associate agreements include specific contractual language requiring specific actions by the lawyer or law firm regarding reporting of security incidents and data breaches.

V. The "Enforcement Rule"

The enforcement provisions under the Final Rule became effective March 26, 2013. As it relates to the enforcement provisions, the Final Rule clarifies the categories of violations under HIPAA and factors used to determine civil money penalties. Significantly, the Final Rule also imposes civil money penalties directly on business associates and their subcontractors and provides for liability of covered entities and business associates for violations caused by their agents. Finally, the Final Rule requires (instead of permitting) HHS to conduct compliance reviews and investigations for certain HIPAA violations and no longer requires HHS to first attempt informal resolution of a violation prior to imposing civil money penalties.

Civil Money Penalties

The Final Rule retains the tiered civil money penalty structure that was implemented in the Interim Final Rule. As a refresher, the tiered system uses increasing penalties based on increasing levels of culpability:

- For a violation in which it is established that the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated such provision, an amount not less than $100 or more than $50,000 for each violation;

- For a violation in which it is established that the violation was due to "reasonable cause" and not to willful neglect, an amount not less than $1,000 or more than $50,000 for each violation;

- For a violation in which it is established that the violation was due to willful neglect but was corrected during the 30–day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, an amount not less than $10,000 or more than $50,000 for each violation;

- For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30–day period beginning on the first date the covered entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, an amount not less than $50,000 for each violation.

The Final Rule clarifies the "state of mind" requirement required for application of the second tier, which provides that a violation occurred when it is established that the violation was due to reasonable cause and not to willful neglect. "Reasonable cause" is now defined as an act or omission in which the covered entity or business associate knew or by reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but which the covered entity or business associate did not act with willful neglect.

The Final Rule also lists numerous factors that HHS considers in determining the amount of a civil money penalty to impose for a HIPAA violation. The factors include (1) the nature and extent of the violation (including the number of individuals affected and the time period), (2) the nature and extent of the harm resulting from the violation (including whether the violation caused physical harm, financial harm or harm to the individual's reputation), (3) the covered entity or business associate's history of prior compliance with HIPAA, and (4) the financial condition of the covered entity or business associate (including the size of the entity, whether the civil money penalty would jeopardize the ability to continue to provide healthcare and whether the entity had financial difficulties that affected its ability to comply).

To avoid civil monetary penalties that rise to the level of "willful neglect" (not less than $10,000 for each violation) lawyers and law firms need to be cognizant of the need to put in place the necessary compliance plan and regularly document its compliance efforts. If OCR

conducts an audit or investigation of a law firm business associate, such law firm should be prepared to respond to OCR's request for documentation of its efforts to comply with HIPAA. If the law firm does not have any "written" documentation of its compliance efforts prior to the incident that lead to the investigation or audit, it is likely that OCR will take a position that the law firm's failure to document its compliance efforts are the equivalent of "willful neglect." What written compliance is recommended? Under the HIPAA Privacy the law firm should document in writing its HIPAA privacy policies and procedures, those individuals within the firm responsible for overseeing compliance efforts, maintain a log or database of business associate and business associate subcontractor relationships, including copies of all business associate agreements, maintain evidence of internal staff training that has been conducted and preserve any internal investigation files related to investigated security incidents or potential breaches of PHI. As for documentation on compliance with the Security Rule, law firms should document in writing its HIPAA security policies and procedures, conduct and maintain a record of risk assessments or risk analysis, reviews of information system security, periodic audit logs, workforce training and training materials and records of any security incident investigations.

Direct Liability for Business Associates and Their Subcontractors

As mentioned above, many of the provisions of HIPAA and the HITECH Act now apply directly to business associates and their subcontractors in substantially the same manner as they apply to covered entities. Consequently, business associates and their subcontractors are subject to civil money penalties for HIPAA violations as mentioned in the preceding section.

Liability for the Acts of Agents

The Final Rule also extends liability to covered entities and business associates when a HIPAA violation is caused by one of their agents. Previously, a covered entity would not be liable for a HIPAA violation caused by an agent as long as the covered entity had met the business associate agreement requirements, did not know the business associate was in violation of the agreement and did not fail to act as required by HIPAA if it was aware of a pattern or practice of violations by the agent. Now, covered entities and business associates can be held liable for the acts of their agents acting within the scope of the agency, regardless of whether the covered entity or business associate did no wrong themselves. HHS acknowledges that whether or not a business associate is an agent of a covered entity will be fact-specific, taking into account the terms of the business associate agreement and the totality of the circumstances involved in the relationship. The biggest factor in determining liability for the acts of agents will be the right or authority of the principal (*e.g.* the covered entity or business associate) to control the conduct of the agent. Other factors HHS will consider include (1) the time, place and purpose of the business associate or subcontractor's conduct, (2) whether the agent engaged in a course of conduct subject to the principal's control, (3) whether the agent engaged in conduct that is of the type a business associate will commonly engage in to accomplish the services provided to the covered entity, and (3) whether the covered entity reasonably expected its business associate to engage in the conduct in question.

VI. Conclusion

Often lawyers and law firms are reluctant to recognize their responsibility as a business associate to comply with HIPAA. However, under today's highly regulated environment, failure to recognize such responsibility and act meaningfully to comply with the requirements may result in significant risk and liability. As discussed above, the Final Rule has significantly increased the financial risk involved in a lawyer or law firm failing to take its compliance obligation under HIPAA seriously. Based on recent actions, audits and settlements, the days of OCR taking an inactive enforcement posture have passed. OCR enforcement activities will continue to increase resulting in the likelihood that your firm will be involved in a HIPAA related investigation or audit.

Good privacy and security practices at your law firm are good business in today's highly data driven world. Lawyers and law firm understand the ethical and business reasons around protecting client confidentiality and client data. The HIPAA privacy and security requirements are largely consistent with these same goals. As such, lawyers and law firms need to dedicate the time, expertise and resources to make sure they are complying with the law.

Lawyer and Law Firm HIPAA Business Associate Compliance Materials, Sample Policies and Procedures and Other Practical Guidance

1. Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act; Final Rule, 78 Fed. Reg. 5566 (January 25, 2013). http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

2. OCR Unofficial Combined Regulations - HIPAA Administration Simplification (Privacy Rule, Security Rule, Enforcement Rule, and Breach Notification Rule), 45 CFR part 160, 162 and 164, Updated as of March 2013. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

3. OCR Sample Business Associate Agreement Provisions (published January 24, 2013). http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

4. OCR Guidance on Risk Analysis under the HIPAA Security Rule, 45 CFR 164.302 – 318. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

5. Sample Law Firm HIPAA Compliance Policy (Attached).

6. Sample HIPAA BAA Subcontractor Letter (Attached).

7. Sample Law Firm Client Business Associate Letter (Attached).

8. Sample Business Associate Agreement (Attached).

SAMPLE LAW FIRM HIPAA COMPLIANCE POLICY

General HIPAA Compliance Policy

Introduction

The Law Firm ("The Firm," "we," "us" or "our") has adopted this HIPAA Compliance Plan in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act of 2009, as well as all implementing regulations.

Assumptions

To the extent we provide services to persons or entities covered by HIPAA (a "HIPAA Client") and in the course of providing such services we create, receive, maintain, or transmit patient health information ("PHI") on behalf of the HIPAA Client, The Firm recognizes its status as a Business Associate under the definitions contained in HIPAA.

To the extent required for Business Associates, The Firm will comply with HIPAA, including entering into a Business Associate Agreement with our HIPAA Clients.

Policy

It is the policy of The Firm to become and to remain in full compliance with all requirements of HIPAA applicable to Business Associates.

It is the policy of The Firm to fully document all HIPAA compliance-related activities and efforts in accordance with our *Documentation Policy*.

All owners, officers, employees, volunteers and other persons whose conduct, in the performance of work for us, is under our direct control (collectively, our "Workforce") are responsible for following this HIPAA Compliance Plan. Workforce members who violate this HIPAA Compliance Plan may be subject to discipline up to and including termination.

Our HIPAA Compliance Plan is reasonably designed, implemented and enforced so that it is effective in preventing, detecting, and remedying the improper use and disclosure of PHI. The specific purposes of our HIPAA Compliance Plan are:

To assist us in identifying PHI.

To assist us in avoiding improper uses and disclosures of PHI.

To assist us in complying with our Business Associate Agreements with HIPAA Clients.

To establish compliance standards and procedures for members of our Workforce that are reasonably capable of reducing the prospect of violating HIPAA.

To appoint a Privacy Officer and a Security Officer who are high-level and trustworthy employees with responsibility to implement and oversee our compliance with the standards and procedures set forth in this HIPAA Compliance Plan.

To effectively communicate the compliance standards, policies and procedures set forth in this HIPAA Compliance Plan to all members of our Workforce by, for example, conducting training and disseminating publications and other materials that explain in a practical manner the HIPAA standards and procedures to be followed.

To take reasonable steps to achieve compliance with the standards, policies and procedures set forth in this HIPAA Compliance Plan by, for example, implementing, monitoring, and auditing systems reasonably designed to detect the improper use and disclosure of PHI.

To establish and publicize a reporting system so that members of our Workforce can report perceived wrongful uses and disclosures of PHI by others without fear of retribution.

To respond appropriately to non-compliance after detection and to prevent recurrence, which may require modifications to this HIPAA Compliance Plan.

Definitions Policy

For purposes of this HIPAA Compliance Plan, the following terms shall have the following meanings:

"Breach" shall mean the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA.

"Business Associate" shall mean a person or entity who performs certain functions or activities on behalf of a "covered entity," as such term is defined by HIPAA (*i.e.*, a healthcare provider, health plan, healthcare clearinghouse or personal health record vendor), which involve the creation, receipt, maintenance, or transmission of PHI on behalf of the covered entity.

"Business Associate Agreement" shall mean an agreement which addresses our use, disclosure, creation, receipt, maintenance, or transmission of PHI on behalf of a HIPAA Client.

"Designated Record Set" shall mean a group of records maintained by or for a HIPAA Client that consist of: (a) the medical records and billing records about individuals; (b) the enrollment, payment, claims adjudication, and case or medical management record systems; or (c) records used, in whole or in part, by or for a HIPAA Client to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a HIPAA Client.

"HIPAA" shall mean: (a) the Health Insurance Portability and Accountability Act of 1996, and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160 and 164, and any subsequent

amendments or modifications thereto, and (b) the HITECH Act, and regulations promulgated thereunder, and any subsequent amendments or modifications thereto.

"HIPAA Client" shall mean one of the following types of persons or entities for which we do work for:

Health Care Providers, which are persons or entities who furnish, bill or are paid for health care services in the normal course of business. (Examples include: physician practices, hospitals, skilled nursing facilities, surgery centers, outpatient rehabilitation facilities, home health agencies, pharmacies, and durable medical equipment providers.)

Health Plans, which are individual or group plans that provide or pay the cost of medical care. (Examples include: HMOs, private health insurers, group health plans, and employee welfare benefit plans.)

Health Care Clearinghouses, which are entities that process PHI in a non-standard HIPAA format or containing non-standard data into a standard format. (Examples include: billing companies, repricing companies, and value added networks.)

Personal Health Record Vendors, which are entities offering or maintaining an electronic record of PHI on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

"HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

"PHI" or "Protected Health Information" shall mean any information, whether oral, written or electronic: (a) that relates to the past, present or future physical or mental condition of an individual; or (b) the provision of health care to an individual; or (c) the past, present or future payment for the provision of health care to an individual; and (d) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, as may be amended, modified or superseded, from time to time.

"Required by Law" shall have the meaning set forth in 45 C.F.R. § 164.103, including, without limitation, a mandate contained in law that compels a HIPAA Client or us to make a use or disclosure of PHI and that is enforceable in a court of law.

"Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

"Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI.

"Security Rules" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164, as may be amended, modified or superseded from time to time.

"Unsecured PHI" shall have the meaning set forth in the HITECH Act, including, without limitation, PHI not secured through the use of encryption, destruction or other technologies and methodologies identified by the Secretary to render such information unusable, unreadable, or indecipherable to unauthorized individuals.

"Workforce" shall include our owners, officers, employees, volunteers and other persons whose conduct, in the performance of work for us, is under our direct control, whether or not they are paid by us.

Privacy Officer Policy

Introduction

This policy governs the designation and duties of a HIPAA Privacy Officer for The Firm. The Privacy Officer shall be a high-level and trustworthy employee of The Firm.

Assumptions

To the extent required for Business Associates, The Firm must comply with HIPAA concerning the assignment of HIPAA responsibilities to a Privacy Officer.

The assignment of overall HIPAA responsibility is an important and integral part of our overall risk management process.

Policy

It is the policy of The Firm to designate a HIPAA Privacy Officer.

The Privacy Officer is responsible for the overall implementation and operation of the privacy of PHI and shall have authority to review all documents and other information relevant to HIPAA activities.

The Privacy Officer shall work closely with the Security Officer in carrying out his/her duties. The position of Privacy Officer and Security Officer may be held by one person.

Privacy activities are a significant component of the Privacy Officer's job description, and therefore his/her performance will be judged, in part, on HIPAA compliance activity and the effectiveness of such activity.

The responsibilities and duties of the Privacy Officer shall focus on the privacy of PHI and include the following:

To assist with the development of our HIPAA Compliance Plan, which sets forth the legal and ethical standards, policies and procedures to be followed by members of our Workforce.

To implement and enforce the standards, policies and procedures set forth in our HIPAA Compliance Plan to ensure our compliance with HIPAA.

To keep apprised of changes to HIPAA. As part of this responsibility, the Privacy Officer will keep track of new regulatory developments, including new HIPAA bulletins and initiatives, many of which can be found at: http://www.hhs.gov/ocr/hipaa.

To communicate the contents of this HIPAA Compliance Plan, new HIPAA legal developments, and new policies and procedures to members of our Workforce through training programs, memoranda, and other appropriate means.

To establish and coordinate regular training programs designed to ensure compliance with the standards and procedures set forth in this HIPAA Compliance Plan and to document the regularity and consistency of such training programs, as well as attendance.

To assist with the development and communication of a system for Workforce members to seek guidance on HIPAA issues and to report suspected violations of our HIPAA Compliance Plan or HIPAA.

To establish a record-keeping system designed to document the ongoing operations of our HIPAA Compliance Plan, including documentation of compliance by all members of our Workforce.

To receive and investigate all complaints relating to possible HIPAA violations and/or violations of our HIPAA Compliance Plan, and to record/document the results of any such complaints.

To review and revise (as necessary) our HIPAA Compliance Plan on at least an annual basis in order to enhance our privacy efforts.

To report to our Governing Body on the operation and implementation of this HIPAA Compliance Plan.

Security Officer Policy

Introduction

This policy governs the designation and duties of a HIPAA Security Officer for The Firm. The Security Officer shall be a high-level and trustworthy employee of The Firm.

Assumptions

To the extent required for Business Associates, The Firm must comply with HIPAA concerning the assignment of PHI security responsibilities to the Security Officer.

The assignment of overall HIPAA security responsibility is an important and integral part of our overall risk management process.

Policy

It is the policy of The Firm to designate a HIPAA Security Officer.

The Security Officer is responsible for the overall implementation and operation of the security of PHI, both electronic and other forms, and shall have authority to review all documents and other information relevant to HIPAA security activities.

The Security Officer shall work closely with the Privacy Officer in carrying out his/her duties. The position of Privacy Officer and Security Officer may be held by one person.

Security activities are a significant component of the Security Officer's job description, and therefore his/her performance will be judged, in part, on PHI security compliance activity and the effectiveness of such activity.

The responsibilities and duties of the Security Officer shall focus on the security of PHI and include the following:

To assist with the development of our HIPAA Compliance Plan, which sets forth the legal and ethical standards, policies and procedures to be followed by members of our Workforce.

To implement and enforce the standards, policies and procedures set forth in our HIPAA Compliance Plan to ensure compliance with the Security Rules.

To keep apprised of changes to the Security Rules. As part of this responsibility, the Security Officer will keep track of new regulatory developments, including new HIPAA bulletins and initiatives, many of which can be found at: http://www.hhs.gov/ocr/hipaa.

To assist the Privacy Officer in the investigation of alleged violations of our HIPAA Compliance Plan and HIPAA, and to work with appropriate parties to handle violations promptly, properly and consistently.

In conjunction with the Privacy Officer, to report to our Governing Body on the operation and implementation of this HIPAA Compliance Plan.

SAMPLE HIPAA BAA SUBCONTRACTOR LETTER

DATE
NAME
ADDRESS

RE: [Insert Matter]

Dear [Name]:

I am enclosing [explain documents enclosed with letter] with regard to the above referenced matter.

Once you have had an opportunity to review these materials, please contact me so that we can schedule a time for you to speak with [Attorney Name] or [Attorney Name] to discuss your findings. Also, please do not prepare any written report at this juncture.

Please note that the enclosed materials constitute the Protected Health Information of one or more individuals, as that term is defined in 45 C.F.R. § 164.501. These materials are subject to the federal privacy, security and breach notification rules issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the related regulations promulgated by the United States Department of Health and Human Services, codified at 45 CFR Parts 160 and 164. In addition, your role as our subcontractor business associate subjects you to certain provisions of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (the "HITECH Act"), including provisions that impose requirements on you with respect to the privacy and security of the enclosed information. Specifically, you are required to abide by the same restrictions and conditions that apply to our use and disclosure of Protected Health Information and are expressly responsible for complying, in all respects, with HIPAA, the HITECH Act and any other applicable state or federal laws governing the confidentiality, privacy, and security of such information.

Please let me know if there is any additional information which you believe may be helpful in your review, and I will attempt to provide you with that information. Should you have any questions or concerns, please do not hesitate to contact me. Thank you for your assistance in this matter.

Sincerely,

[Insert Name]

Enclosures

SAMPLE LAW FIRM CLIENT
BUSINESS ASSOCIATE AGREEMENT LETTER

INSTRUCTIONS:
BEFORE SIGNING ANY BAA REQUESTED BY A CLIENT THE LAW FIRM'S HIPAA PRIVACY COMMITTEE MUST ASSESS WHETHER ONE IS NECESSARY AND REQUIRED TO BE SIGNED.

THE THREE REQUIREMENTS UNDER HIPAA THAT QUALIFY OUR FIRM AS A BUSINESS ASSOCATE UNDER ARE AS FOLLOWS:
1. IS THE CLIENT A HEALTH CARE PROVIDER, HEALTH INSURANCE COMPANY OR HEALTH TRANSACTIONAL COMPANY AS DEFINED UNDER HIPAA? IF SO THE CLIENT IS A "COVERED ENTITY" UNDER HIPAA.
2. DO WE PROVIDE A SERVICE FOR OR ON BEHALF OF THE COVERED ENTITY CLIENT? (LEGAL SERVICES QUALIFY – IN MOST CASES THIS WILL BE YES)
3. AS A PART OF OUR REPRESENTATION OF CLIENT WILL THE CLIENT PROVIDE US WITH ACCESS OR COPIES OF PHI (MEDICAL/HEALTH INFO) THAT THE CLIENT IS RESPONSIBLE FOR MAINTAINING. IF SO, BAA IS REQUIRED. IF NO, NO BAA IS NOT REQUIRED.

[EXAMPLE – WE ARE ASKED TO REPRESENT A PHYSICIAN IN MEDICAL MALPRACTICE CASE AND ARE PROVIDED MEDICAL RECORDS. YES, BAA IS REQUIRED. HOWEVER, IF WE ARE ASKED TO REPRESENT THE PHYSICIAN IN AN EMPLOYMENT CASE AND GET MEDICAL RECORDS OF THE EMPLOYEE. NO, BAA IS NOT REQUIRED.]

DATE

CLIENT
ADDRESS

RE: Business Associate Agreement – [Client Name]

Dear _____:

[Attorney's Name] forwarded to me your request that our firm execute a Business Associate Agreement under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).

Since our law firm provides [plans to provide] professional legal services to you and as a part of our representation you will be sharing with us certain medical and health related information known under HIPAA as protected health information we are required to enter into a Business Associate Agreement. We further understand that HITECH imposes additional HIPAA Privacy Rule, HIPAA Security Rule, and new breach notification requirements on covered entities and business associates.

As a client of our firm, we are providing you with our standard Business Associate Agreement so that we can appropriately comply with these rules. We have tailored this Business Associate Agreement to address specific needs unique to the professional legal and business relationship that [Law Firm Name] has with its clients. I have executed the Business Associate Agreement on behalf of our firm. Once you have executed the Business Associate Agreement, please return a copy of the fully executed document to the following address:

Attn: [Name], [Title]
ADDRESS

We value you as a client of our firm and hope that you will find that us providing you with this agreement simplifies your HIPAA compliance efforts. If you have any questions, please contact me at _____.

Sincerely,

Name
Title

Enclosure
cc: [Attorney's Name]

SAMPLE BUSINESS ASSOCIATE AGREEMENT

Business Associate Agreement

This Business Associate Agreement ("Agreement") is dated and effective on _____, 2014, between **[COVERED ENTITY]** ("Covered Entity") and **[BUSINESS ASSOCIATE]** ("Business Associate").

WHEREAS, the Covered Entity and the Business Associate have entered a business arrangement, including providing the following services: _____ [NOTE: ADD DESCRIPTION OF THE SPECIFIC SERVICE] ("Services").

WHEREAS, as a result of providing such Services, the Business Associate may be considered a "business associate" of the Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996, as amended ("**HIPAA**"), and including all pertinent regulations issued by the U.S. Department of Health and Human Services, as either have been amended by the Health Information Technology for Economic & Clinical Health Act and the Omnibus Final Rule (78 FR 5566) **(**"**HITECH" Act**"). The business relationship or arrangement between the Covered Entity and the Business Associate may involve the disclosure of Protected Health Information, as hereinafter defined, by the Covered Entity to the Business Associate that is subject to the federal privacy and security regulations issued pursuant to the HIPAA and the HITECH Act;

WHEREAS, the Covered Entity and the Business Associate mutually agree to the terms of this Agreement, which sets forth the obligations of the parties as required by the Standards for Security and Privacy of Individually Identifiable Information, codified at 45 C.F.R. §§ 160 through 164 ("**Security and Privacy Regulations**"), as applicable, under the HIPAA and the HITECH Act;

WHEREAS, the Security and Privacy Regulations require that the Covered Entity and the Business Associate enter into a written contract or other arrangement that meets the applicable requirements of 45 C.F.R. §§ 164.314 and 164.504.

NOW THEREFORE, the Parties, hereby agree as follows:

1. Definitions.

a. Except as otherwise defined in this Agreement, all capitalized terms used in this Agreement shall have the meanings set forth in the Security and Privacy Regulations.

b. "**Breach**" shall have the same meaning as the term "breach" in 45 C.F.R. §164.402.

c. "**Business Associate**" shall have the same meaning as the term "business associate" in 45 C.F.R. § 160.103.

d. "**Covered Entity**" shall have the same meaning as the term "covered entity" in 45 C.F.R. § 160.103.

e. **"Designated Record Set"** shall have the same meaning as the term "designated record set" in 45 C.F.R. §164.501.

f. "**Electronic Protected Health Information**" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. §160.103, limited to the Protected Health Information created, received, maintained or transmitted by or on behalf of the Covered Entity to the Business Associate as contemplated by this Agreement.

g. "**HIPAA Breach Notification Rule**" shall mean the federal breach notification regulations, as amended from time to time, issued under HIPAA and set forth in 45 C.F.R. Part 164 (Subpart D).

h. "**Individual**" shall have the same meaning as the term "individual" in 45 C.F.R. §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g).

i. "**Privacy Rule**" shall mean the federal privacy regulations, as amended from time to time, issued under the HIPAA and the HITECH Act and set forth in 45 C.F.R. Parts 160 and 164 (Subparts A & E).

j. "**Security Rule**" shall mean the federal security regulations, as amended from time to time, issued under the HIPAA and the HITECH Act and set forth in 45 C.F.R. Parts 160 and 164 (Subparts A & C).

k. "**Subcontractor**" shall have the same meaning as the term "subcontractor" in 45 C.F.R. §160.103.

l. "**Protected Health Information**" shall have the same meaning as the term "protected health information" in 45 C.F.R. §160.103, limited to the Protected Health Information created, received, maintained or transmitted by or on behalf of the Covered Entity to the Business Associate as contemplated by this Agreement.

2. Uses and Disclosures of Protected Health Information by the Business Associate.

a. The Business Associate agrees to use or disclose Protected Health Information only as specifically permitted or required by this Agreement or as required by law. The Business Associate shall not use or disclose Protected Health Information for any other purpose or in any other manner.

b. The Business Associate may, if necessary, use or disclose Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate; provided, that (i) any such disclosure is required by law; or (ii) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person or party immediately notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited by this Agreement, the Business Associate may use Protected Health Information to provide data aggregation services to the Covered Entity.

d. The Business Associate may de-identify any and all Protected Health Information that it obtains from the Covered Entity, but only if such de-identification is accomplished in accordance with the requirements of 45 C.F.R. § 164.514(a) and (b).

3. Obligations of the Business Associate.

a. The Business Associate shall use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic Protected Health Information, to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement.

b. The Business Associate shall report to the Covered Entity (i) any use or disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(C); or (ii) any Security Incident of which the Business Associate becomes aware in accordance with 45 C.F.R. § 164.314(a)(2)(i)(C).

c. The Business Associate shall notify the Covered Entity without unreasonable delay after the Business Associate's discovery of any incident that involves an unauthorized acquisition, access, use, or disclosure of Protected Health Information. In the event of an incident that is required to be reported under the HIPAA Breach Notification Rule, the Covered Entity shall elect in its sole discretion whether the Covered Entity, the Business Associate or a third party shall be responsible for conducting an investigation of the incident and providing any required notices.

d. The Business Associate shall ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree to the same restrictions and conditions that apply through this Agreement to the Business Associate with respect to such Protected Health

Information in accordance with 45 C.F.R. 164.502(e)(1)(ii) and 45 C.F.R. 164.308(b)(2).

e. The Business Associate shall provide access to the Covered Entity to Protected Health Information in a Designated Record Set, or, if requested by the Covered Entity, to an Individual or the Individual's designee, all in accordance with the requirements under 45 C.F.R. § 164.524.

h. The Business Associate shall make available and make any amendments to Protected Health Information in a Designated Record Set, or, if requested by the Covered Entity, from an Individual or the Individual's designee, all in accordance with the requirements of 45 C.F.R. § 164.526.

i. The Business Associate shall make available to the Covered Entity information to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information, or, if requested by the Covered Entity, to make that information available directly to an Individual, all in accordance with 45 C.F.R. § 164.528.

j. The Business Associate shall notify the Covered Entity in writing after the Business Associate's receipt directly from an Individual of any request for access to or amendment of Protected Health Information, or an accounting of disclosures, as contemplated by this Agreement.

f. To the extent that the Business Associate is to carry out the Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, the Business Associate shall comply with the requirements of that section that apply to the Covered Entity in the performance of such obligations.

k. The Business Associate shall provide reasonable access to its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information, to the Secretary for purposes of determining the Covered Entity's or the Business Associate's compliance with the HIPAA, the HITECH Act and the Security and Privacy Regulations.

l. The Business Associate shall request, use and/or disclose only the minimum amount of Protected Health Information necessary to accomplish the purpose of the request, use or disclosure in accordance with 45 C.F.R. §§ 164.502(b) and 164.514(d).

m. The Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information as prohibited by 45 C.F.R. § 164.502(a)(5)(ii).

n. The Business Associate shall not make or cause to be made any communication about a product or service that is prohibited by 45 C.F.R. §§ 164.501 and 164.508(a)(3).

o. The Business Associate shall not make or cause to be made any written fundraising communication that is prohibited 45 C.F.R. § 164.514(f).

p. The Business Associate shall take all reasonable steps, at the request of the Covered Entity, to comply with requests by Individuals not to disclose Protected Health Information to a Health Plan in accordance with 45 C.F.R. § 164.522(a).

4. Term and Termination.

a. The term of this Agreement shall commence upon the effective dated and shall terminate (i) at the conclusion of Business Associate providing the Service to the Covered Entity; (ii) by mutual written agreement of the Parties; or (iii) on the date that the Covered Entity terminates as authorized in this section, whichever is sooner.

b. Notwithstanding anything in this Agreement to the contrary, if the Covered Entity knows of a pattern of activity or practice of the Business Associate that constitutes a material breach or violation of this Agreement, then the Covered Entity shall provide written notice of the breach or violation to the Business Associate that specifies the nature of the breach or violation. The Business Associate must cure the breach or end the violation on or before 30 days after receipt of the written notice. In the absence of a cure reasonably satisfactory to the Covered Entity within the specified timeframe, or in the event the breach is reasonably incapable of cure, then the Covered Entity may, terminate this Agreement.

c. Upon termination of this Agreement for any reason, the Business Associate, with respect to Protected Health Information received from the Covered Entity, or created, maintained, or received by the Business Associate on behalf of the Covered Entity, shall:
    i. Retain only that Protected Health Information which is necessary for the Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
    ii. Return or destroy, if feasible, all remaining Protected Health Information received from the Covered Entity, or created, maintained, or received by the Business Associate on behalf of the Covered Entity, that the Business Associate maintains in any form;
    iii. Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic Protected Health Information to prevent use or disclosure of the Protected Health Information, other than as provided for in this section, for as long as the Business Associate retains the Protected Health Information;
    iv. Not use or disclose the Protected Health Information retained by the Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out above which applied prior to termination; and

v. Return or destroy, if feasible, all Protected Health Information retained by the Business Associate when it is no longer needed by the Business Associate for its proper management and administration or to carry out its legal responsibilities.

d. The obligations of the Business Associate under this section shall survive the termination of this Agreement and shall continue to bind the Business Associate, its agents, employees, contractors, successors, and assigns as set forth herein.

5. Miscellaneous.

a. **Entire Agreement**. This Agreement constitutes the entire agreement of the Parties relating to the Business Associate's use and/or disclosure of Protected Health Information.

b. **Regulatory References**. Any references in this Agreement to a section in the HIPAA, the HITECH Act or the Security and Privacy Regulations means the section as in effect or as amended.

c. **Interpretation**. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA, the HITECH Act or the Security and Privacy Regulations.

d. **Amendment and Assignment**. This Agreement may be amended or modified only by written agreement made by and between the Parties. No party may assign its respective rights and obligations under this Agreement without the prior written consent of the non-assigning party.

e. **Compliance**. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event that the Covered Entity believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA, the HITECH Act or the Security and Privacy Regulations, the Covered Entity shall notify the Business Associate in writing. For a period of up to 30 days, the Parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such 30 day period, the Agreement fails to comply with the requirements of HIPAA, then the Covered Entity has the right to terminate this Agreement upon written notice to the Business Associate.

f. **Mediation and Arbitration**. The parties agree to mediate any dispute or claim, including a breach, arising out of or relating to this Agreement, by mutually agreeing on an independent mediator or mediation service, including the mediation services offered by the American Health Lawyers Association. In the event that the parties are unable, within 30 days after written demand for

mediation, to agree to a mutually acceptable mediation or mediation service or mutually agree to an extension of time to mediate and result the dispute or claim, the dispute or claim shall be settled by arbitration administered by and in accordance with the rules of the American Health Lawyers Association. The place of arbitration shall be _____. Judgment on the award rendered by the arbitrator may be entered in any court having jurisdiction thereof.

g. **Legal Fees**. In the event that the Covered Entity fails to proceed with mediation or arbitration, unsuccessfully challenges the arbitrator's award, or fails to comply with the arbitrator's award or mediated settlement, the Business Associate shall be entitled to costs, expenses and reasonable attorneys' fees in connection with such collection action as well as the reasonable value of the Business Associate's time, computed according to our prevailing fee schedules and expense policies.

h. **Choice of Law**. The laws of the State of _____ (without giving effect to its conflicts of law principals) govern all matters under this Agreement.

IN WITNESS WHEREOF, the Parties have executed this Business Associate Agreement.

COVERED ENTITY

_____
Print Company Name

By: _____

Its: _____

BUSINESS ASSOCIATE

[BUSINESS ASSOCIATE]

By: _____

Its: _____