KREVOLIN | HORST LLC

www.khlawfirm.com

MEMORANDUM

DATE: November 10, 2011

TO:

FROM: Krevolin & Horst, LLC

RE: HIPAA Obligations of Business Associates

In connection with the launch of your hosted application service focused on practice and revenue cycle management, you have inquired as to your obligations under Health Insurance Portability and Accountability Act (**"HIPAA"**). As a provider of claims processing or administration services, data processing services, billing, and or practice management services, you will be deemed a Business Associate of each "health care provider" that is a user of your services. This memorandum outlines the primary obligations of Business Associates under HIPAA and the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (**"HITEC"**). HITEC was enacted to promote the adoption and meaningful use of health information technology. Subtitle D of HITEC addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Definitions

A **"Covered Entity"** under HIPAA is either a "health plan," "health care clearinghouse" or a "health care provider", each of which has a detailed definition under HIPAA.

A **"Business Associate"** of a Covered Entity under HIPAA performs certain functions or activities that involve the use or disclosure of "Protected Health Information" on behalf of, or provides services to, a Covered Entity. These functions and activities include claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, billing, benefits management, practice management, and repricing. Business associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial services.

"Protected Health Information" or **"Protected Health Information"** is individually identifiable health information received from or created or received on behalf of a Covered Entity.

Obligations of Business Associates under HIPAA and HITEC

As a result of the adoption of HITEC, the HIPAA privacy and security requirements directly apply to Business Associates. Business Associates are subject to the same civil and criminal penalties as Covered Entities.

One Atlantic Center | 1201 W. Peachtree St., NW | Suite 3250 | Atlanta, GA 30309 | 404-888-9700 | Fax 404-812-3101

The HIPAA Privacy Rule

The Privacy Rule protects all Protected Health Information held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral. Covered Entities and their Business Associates must develop policies and procedures that reasonably limit its disclosures of and requests for, Protected Health Information for "payment" and health care operations to the minimum necessary. ***"Payment"*** encompasses the various activities to obtain payment or be reimbursed for services. Covered Entities and their Business Associates are required to develop and implement *written privacy policies and procedures* that are consistent with the Privacy Rule. Covered Entities and their Business Associates must *designate a privacy official* responsible for developing and implementing privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the Covered Entity's privacy practices.

The HIPAA Security Rule

The HIPAA Security Rule requires Covered Entities and their Business Associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-Protected Health Information. Specifically, Covered Entities and their Business Associates must:

- Ensure the confidentiality, integrity, and availability of all e-Protected Health Information they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

As used in the Security Rule:

"Confidentiality" means that e-Protected Health Information is not available or disclosed to unauthorized persons.

"Integrity" means that e-Protected Health Information is not altered or destroyed in an unauthorized manner, and

"Availability" means that e-Protected Health Information is accessible and usable on demand by an authorized person.

Covered Entities and Business Associates must review and modify their security measures to continue protecting e-Protected Health Information in a changing environment.

Risk Analysis and Management

The Administrative Safeguards provisions of the Security Rule require Covered Entities and their Business Associates to perform risk analysis as part of their security management processes. Risk Analysis includes, but is not limited to, the following activities:

- Evaluation of the likelihood and impact of potential risks to e-Protected Health Information;
- Implementation appropriate security measures to address the risks identified in the risk analysis;
- Document the chosen security measures and, where required, the rationale for adopting those measures; and
- Maintain continuous, reasonable, and appropriate security protections.

Risk analysis should be an ongoing process, in which Covered Entities and their Business Associates regularly review records to track access to e-Protected Health Information and detect security incidents, periodically evaluate the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-Protected Health Information.

Administrative Safeguards

Security Process. Covered Entities and their Business Associates must identify and analyze potential risks to e-Protected Health Information, and implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Security Personnel. Covered Entities and their Business Associates must designate a security official who is responsible for developing and implementing its security policies and procedures.

Access Management. The Security Rule requires a Covered Entities and their Business Associates to implement policies and procedures for authorizing access to e-Protected Health Information only when such access is appropriate based on the user or recipient's role (role-based access).

Workforce Training and Management. Covered Entities and their Business Associates must provide for appropriate authorization and supervision of workforce members who work with e-Protected Health Information. A Covered Entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Evaluation. A Covered Entities and their Business Associates must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

***Facility Access and Control*.** Covered Entities and their Business Associates must limit physical access to its facilities while ensuring that authorized access is allowed.

***Workstation and Device Security*.** Covered Entities and their Business Associates must implement policies and procedures to specify proper use of and access to workstations and electronic media. Covered Entities and their Business Associates also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic Protected Health Information (e-Protected Health Information).

Technical Safeguards

***Access Control*.** Covered Entities and their Business Associates must implement technical policies and procedures that allow only authorized persons to access electronic Protected Health Information (e-Protected Health Information).[24]

***Audit Controls*.** Covered Entities and their Business Associates must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-Protected Health Information.

***Integrity Controls*.** Covered Entities and their Business Associates must implement policies and procedures to ensure that e-Protected Health Information is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-Protected Health Information has not been improperly altered or destroyed.

***Transmission Secu*rity.** A Covered Entities and their Business Associates must implement technical security measures that guard against unauthorized access to e-Protected Health Information that is being transmitted over an electronic network.

Organizational Requirements

***Responsibilities*.** If a Covered Entity knows of an activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation, the Covered Entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-Protected Health Information. Likewise if a Business Associate knows of an activity or practice of a Covered Entity that constitutes a material breach or violation of the Covered Entity's obligations, the Business Associate must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-Protected Health Information.

Breach Notification Rule

Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITEC) Act by requiring HIPAA

Covered Entities and their Business Associates to provide notification following a breach of unsecured Protected Health Information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITEC Act.

Definition of Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the Protected Health Information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach."

- Unintentional acquisition, access, or use of Protected Health Information by a workforce member acting under the authority of a Covered Entity or Business Associate.

- Inadvertent disclosure of Protected Health Information from a person authorized to access Protected Health Information at a Covered Entity or Business Associate to another person authorized to access Protected Health Information at the Covered Entity or Business Associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the Covered Entity or Business Associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Covered entities and Business Associates must only provide the required notification if the breach involved unsecured Protected Health Information. Unsecured Protected Health Information is Protected Health Information that ***has not*** been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance.

Protected Health Information is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

- Electronic Protected Health Information has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

- Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

- Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

- The media on which Protected Health Information is stored or recorded has been destroyed in one of the following ways:

  - Paper, film, or other hard copy media have been shredded or destroyed such that the Protected Health Information cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

  - Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the Protected Health Information cannot be retrieved.

Breach Notification Requirements

If a breach of unsecured Protected Health Information occurs at or by a Business Associate, the Business Associate must notify the Covered Entity following the discovery of the breach. A Business Associate must provide notice to the Covered Entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the Business Associate should provide the Covered Entity with the identification of each individual affected by the breach as well as any information required to be provided by the Covered Entity in its notification to affected individuals.

Obligations of Covered Entities with respect to Business Associates

HIPAA requires that a Covered Entity have a written agreement with its Business Associate. The Covered Entity must, through such a written agreement, obtain "satisfactory assurance" from the Business Associate that the Business Associate will "appropriately safeguard" Protected Health Information the Covered Entity discloses to the Business Associate. The following points summarize the minimum required obligations in a "standard" Business Associate Agreement found in the federal regulations.

Business Associates must:

• Report any unauthorized use or disclosure of the Protected Health Information to the Covered Entity.

• Report any security incident to the Covered Entity.

• Not use or further disclose the Protected Health Information other than as permitted or required by the agreement or as required by law.

• Obligate their agents and subcontractors to agree to the same restrictions and conditions that apply to the Business Associate, and the Business Associate their agents and subcontractors must agree to implement reasonable and appropriate safeguards for the protection of electronic Protected Health Information.

• Make the Protected Health Information available in connection with individuals' rights under federal law to access their Protected Health Information. If a Business Associate maintains an electronic health record, it must agree to provide such information in electronic format.

• Make the Protected Health Information available for amendment and incorporate any amendments in connection with individuals' rights under federal law to seek amendment of their Protected Health Information.

• Make available the information required to provide an accounting of disclosures of Protected Health Information to individuals in accordance with their rights under federal law to obtain such an accounting.

• Make their internal practices, books, and records relating to the use and disclosure of the Protected Health Information available to the federal government for purposes of determining the Covered Entity's compliance with HIPAA.

• Return or destroy all Protected Health Information, if feasible, at the termination of the agreement, or, if return or destruction is not feasible, Business Associates must continue to protect the Protected Health Information even after termination.

• Comply with the HIPAA Security Rule.

• Agree to report any access, use, or disclosure of Protected Health Information not permitted by the Agreement, and any breach of Protected Health Information of which it becomes aware without unreasonable delay and in no case later than 60 calendar days after discovery.

• Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the agreement.

• Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic Protected Health Information.

Business Associate Agreements - Negotiating Points.

The most common, and most controversial, non-required provision is an indemnity clause. Many covered entities are attempting to obtain full indemnity from damages caused by a Business Associate's breach of the agreement. The HIPAA Privacy Rule does not require, or even discuss, indemnity clauses or damages due to disclosures of protected information. The effect or legal validity of these indemnity clauses is unclear, as the HIPAA Privacy Rule is still too new to have spawned civil lawsuits. The evaluation of these indemnity agreements is no different for a Business Associate agreement than for any other business contract.

Another common provision that is not required under the HIPAA Privacy Rule is a provision allowing a Covered Entity to examine the books and premises of the Business Associate for satisfaction that the information will be protected. There is no requirement for this type of examination in the HIPAA Privacy Rule, and a Covered Entity has no duty to ensure the protection of information by the Business Associate beyond entering into a Business Associate agreement. This provision has typically been requested by large and powerful covered entities, and it is unclear at this point whether any of the covered entities have an intention to undertake a thorough investigation.

Another interesting provision that has been included in some agreements specifies that the Covered Entity retains all property rights to the protected information disclosed to the Business Associate. This may be especially important to groups that have a patient database that would be desirable to third-party marketers. Some Business Associates have maintained that they have the right to strip the individually identifiable information from the protected information and sell the collective "de-identified" data to a third party. HIPAA does create a process for de-identifying protected information for unfettered use by a Covered Entity, but the regulation is unclear as to whether a Business Associate has a similar right. Nonetheless, by retaining property rights to the protected information, some covered entities are protecting themselves and their patients from such uses.

HIPAA Enforcement. Penalties

HIPAA authorizes monetary fines of $1,000 per violation up to an annual maximum of $25,000. For criminal violations, the fines can be as much as $250,000 and 10 years in prison.