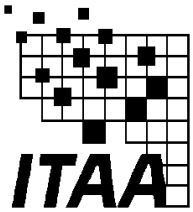

HIPAA AND ITS LEGAL IMPLICATIONS FOR HEALTH CARE INFORMATION TECHNOLOGY SOLUTION PROVIDERS

A White Paper Jointly Issued By The Rotbert Law Group, LLC and the Information Technology Association of America

April 9, 2004

HIPPA AND ITS LEGAL IMPLICATIONS FOR HEALTH CARE INFORMATION TECHNOLOGY SOLUTION PROVIDERS

INTRODUCTION

The health care industry is undergoing a radical revolution through the rapid adoption of information technology (IT) solutions to meet the challenges of regulatory burdens, cost reduction, and patient care. Some of these IT solutions include computerized physician order entry initiatives, electronic medical records, and electronic claims processing. A recent IDC study projected that IT spending in the United States among health care providers will increase from $15.1 billion in 2002 to $17.3 billion in 2007. The demand for innovative IT solutions and increased spending creates a tremendous opportunity for health care IT solution providers. However, the health care sector is also subject to an onerous regulatory framework that health care IT solution providers must navigate proficiently to be successful.

Part of that regulatory framework is the Health Insurance Portability and Accountability Act (HIPAA). Health plans, health care clearinghouses, and health care providers who transmit health information in electronic form ("covered entities") must be in compliance with HIPAA or face the possibility of significant fines or even jail time. Consequently, health care IT solution providers must understand HIPAA and its implications.

This white paper provides an overview of HIPAA's legal implications for health care IT solution providers such as software vendors, application service providers ("ASPs"), outsourcers, and systems integrators.

HIPAA – What it is; How it works

HIPAA was enacted in 1996 as part of a broad congressional attempt at incremental health care reform. The law required the United States Department of Health and Human Services (DHHS) to develop standards and requirements for the maintenance and transmission of health information. DHHS's rules and regulations focus on four primary areas: privacy, security, transaction standards and code sets, and unique identifiers.

The Privacy Rule requires covered entities to guard against misuse of personally identifiable health information and limit the sharing of such information. The Privacy Rule also grants consumers significant rights regarding the use and disclosure of their health information.

The Security Rule requires covered entities to implement basic safeguards to protect electronic protected health information ("PHI") from unauthorized access, alteration, deletion, and transmission. The security standards define the administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI.

The rule relating to standard transactions and code sets was designed to improve the Medicare and Medicaid programs and the health care industry in general by enabling efficient electronic transmission of certain health information.

HIPAA also requires unique identifiers for providers, health plans, payors, and patients. These unique identifiers will increase the speed of payments, reduce costs, and promote coordination among health care entities.

Although health care IT solution providers are not expressly mandated to comply with HIPAA, HIPPA should still be a primary focus. A failure to properly navigate HIPAA could dramatically impact a health care IT solution provider's business resulting in a failure to attract new customers, loss of existing customers, and even civil or criminal liability from improper handling of PHI.

BUSINESS ASSOCIATE CONTRACTS

Most health care IT solution providers' first direct exposure to HIPPA will occur through what are termed "Business Associate Contracts" under HIPAA. In certain situations, the HIPAA Privacy Rule and Security Rule both require Business Associate Contracts between covered entities and health care IT solution providers.

Privacy Rule

Under the Privacy Rule, the Business Associate Contract establishes the health care IT solution provider's permitted uses and disclosures of PHI. If a Business Associate Contract is required under the Privacy Rule, it must set forth the manner in which the health care IT solution provider may use and disclose PHI.

The Privacy Rule also requires that the Business Associate Contract contain an express agreement that the health care IT solution provider will use appropriate safeguards to prevent use or disclosure of the PHI, other than as provided for in the Business Associate Contract, and that the health care IT solution provider will not use or further disclose the PHI other than as permitted or required by the contract or as required by law. The Business Associate Contract should also require the health care IT solution provider to report to the covered entity any use or disclosure of the PHI not provided for by the contract of which the health care IT solution provider becomes aware.

The Privacy Rule also imposes certain requirements on the availability of, access to, and accounting of PHI. Specifically, the Business Associate Contract must require the health care IT solution provider to:

1. make an individual's PHI available for inspection and copying;

2. make PHI available for amendment and then incorporate any amendment in accordance with the individual's right to amend health records;

3. make available the information required to provide an accounting of disclosures in accordance with the Privacy Rule requirements;

4. make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the health care IT solution provider on behalf of the covered entity available to DHHS for purposes of determining the covered entity's compliance with HIPAA.

The Business Associate Contract must also require the health care IT solution provider to ensure that any agents or subcontractors to whom the health care IT solution provider provides PHI (received from, or created or received by the health care IT solution provider on behalf of, the covered entity) agrees to the same restrictions and conditions that apply to the health care IT solution provider with respect to such PHI.

The Privacy Rule permits the covered entity and the health care IT solution provider to agree that the health care IT solution provider may use PHI for its management, administration, and legal responsibilities. When the information is disclosed by the health care IT solution provider for proper management or administration, the health care IT solution provider should obtain reasonable assurances from such persons to whom the PHI is disclosed that the information will be held in confidence and only further disclosed if required by law or for the purpose for which the information was disclosed. In addition, the health care IT solution provider should obtain reasonable assurances from any such persons that they will notify the health care IT solution provider immediately of any instance where the person becomes aware that the information's confidentiality has been breached. Although such a provision is optional for the Business Associate Contract, a health care IT solution provider may consider this provision necessary to facilitate its business and remain competitive.

In the Business Associate Contract, the parties may agree that the health care IT solution provider can provide data aggregation or mining relating to the health care operations of the covered entity. The covered entity may, for example, want to contract with a health care IT solution provider to conduct quality assurance and comparative analyses involving other health care providers' PHI. Without this exemption, such data aggregation would be prohibited because a covered entity cannot generally disclose PHI to another covered entity, except under limited circumstances.

The Privacy Rule requires the Business Associate Contract to provide that the health care IT solution provider will agree to terminate the contract if the health care IT solution provider has violated any material term of the contract. The Privacy Rule regulations recognize that in some instances it may not be feasible for the covered entity to terminate a contract with a health care IT solution provider because there is no viable alternative. The fact that an alternative may be less convenient or more costly does not mean that an alternative is not feasible. No viable alternative may be present when the covered entity has entered into a large complex IT transaction with a health care IT solution provider. For situations where no viable alternatives exist, the health care customer must notify DHHS of the violation.

The Business Associate Contract must also provide that at termination of the contract, the health care IT solution provider will, if feasible, return or destroy all PHI received from the covered entity or created by the health care IT solution

provider on behalf of the covered entity and retain no copies. If return or destruction is not feasible, the health care IT solution provider must agree to extend the protections of the contract to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. The Privacy Rule regulations recognize there may be situations where the return or destruction of PHI is not feasible. For example, in the case of electronic back-up files, the health care IT solution provider cannot be expected to destroy entire electronic back-up files as those back-up files may contain information related to any number of different clients and to destroy or erase select portions of such back-up files may not be practical. This requirement on contract termination implicitly requires the health care IT solution provider to have its down stream providers also agree to return or destroy all PHI they have received from the health care IT solution provider.

Security Rule

The Security Rule also mandates the use of a Business Associate Contract. The Security Rule allows a covered entity to permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. A Business Associate Contract between a covered entity and a health care IT solution provider under the Security Rule, must provide that the health care IT solution provider will (1) 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 the covered entity; (2) ensure that any agent, including a subcontractor, to whom it provides PHI agrees to implement reasonable and appropriate safeguards to protect the PHI; (3) report to the covered entity any security incident of which it becomes aware; (4) make its policies and procedures, and documentation relating to such safeguards, available to the Secretary of DHHS for purposes of determining the covered entity's compliance with the Business Associate Contract requirements of the Security Rule; and (5) authorize termination of the contract by the covered entity if the covered entity determines that the health care IT solution provider violated a material term of the contract.

Timing Considerations

By April 14, 2004, all covered entities must have Business Associate Contracts with their business associates that contain the mandatory provisions required by the Privacy Rule. The Privacy Rule provided for a transition period for a covered entity that had an existing written agreement with a business associate prior to October 15, 2002 and the agreement was not renewed or modified between October 15, 2002 and April 14, 2003, the compliance date of the Privacy Rule. These existing or roll-over agreements (agreements that renew automatically without any change in terms or other action by the parties) are deemed compliant with the Business Associate Contract requirement until such agreement is renewed or modified after April 14, 2003 or until April 14, 2004, whichever is sooner. At such time, the covered entity must enter into an agreement with the business associate that satisfies the Business Associate Contract requirements of the Privacy Rule.

The Security Rule Business Associate Contract provisions do not become mandatory until April 21, 2005. However, as a covered entity enters into a Business Associate Contract with health care IT solution provider to comply with the Privacy Rule and the parties would be required to enter into a Security Rule Business Associate Contract, it is recommended that they include the required Security Rule Business Associate Contract provisions with an effective date of April 21, 2005. This step will eliminate the possibility that a covered entity will insert optional provisions into the Business Associate Contract closer to the implementation date of the Security Rule that create additional burdens for the health care IT solution provider. In addition, it will allow ample time for the health care IT solution provider to implement policies and procedures to comply with its Business Associate Contract obligations under the Security Rule.

Optional Provisions

The Privacy Rule creates room for negotiations between the covered entity and the health care IT solution provider on a number of open Business Associate Contract issues. Some of these open issues that the health care IT vendor and the covered entity may want to consider include:

1. The timing and manner of providing access to PHI, accounting for disclosures of PHI, and making amendments to PHI;

2. The process for access to the health care IT solution provider's practices, books, and records in connection with PHI to determine the covered entity's compliance with the Privacy Rule;

3. Allocating responsibility for the cost of mitigating harmful effects of any improper use of PHI;

4. Whether the health care IT solution provider should assist covered entities with Privacy Rule obligations;

5. Determining whether return or destruction of PHI is feasible at the termination of the contract.

In relationships where the covered entity has superior bargaining power, the covered entity may insist on including additional obligations on the health care IT solution provider. A health care IT solution provider should carefully scrutinize every proposed Business Associate Contract from a covered entity to identify whether the Business Associate Contract imposes additional requirements beyond those mandated by HIPPA. If the Business Associate Contract does impose such additional obligations, the health care IT solution provider should evaluate whether it will agree to assume such additional risks and obligations and whether it has structured its pricing model to appropriately compensate for bearing such additional risks and obligations.

From a contract management standpoint, it is far better for a health care IT solution provider to propose a standard Business Associate Contract to its existing or potential health care customers, than to have those customers

propose Business Associate Contracts of their own. If left to its own devices, a covered entity may place more onerous burdens on its health care IT solution provider in the Business Associate Contract and thereby alter the health care IT solution provider's cost structure. In addition, the covered entity may omit provisions that are important to the health care IT solution provider. Consequently, a health care IT solution provider should take the initiative to prepare contracts that contain the necessary Business Associate Contract provisions and offer those to customers.

WHEN IS A BUSINESS ASSOCIATE CONTRACT NECESSARY?

In many instances, it is readily apparent that the relationship between the covered entity and the health care IT solution provider requires a Business Associate Contract. In other situations, it may not be clear whether a Business Associate Contract is required. In those situations, the health care IT solution provider should closely scrutinize its offering to assess whether it can legitimately take the position that a Business Associate Contract is not required, because a Business Associate Contract imposes significant risks and burdens on the health care IT solution provider.

Many covered entities have taken the approach of attempting to have every vendor execute a Business Associate Contract. Covered entities are motivated to err on the side of executing Business Associate Contracts because, if it is found that a Business Associate Contract was required between a covered entity and a business associate, but one was not in place, the covered entity would be violating HIPPA. Moreover, there is no downside for a covered entity to execute a Business Associate Contract with a vendor. Consequently, there is an inherent tension between a covered entity seeking a Business Associate Contract and a health care IT solution provider's desire to avoid a Business Associate Contract.

The Privacy Rule requires the use of a Business Associate Contract between a covered entity and a health care IT solution provider where the covered entity is disclosing PHI to a health care IT solution provider who performs a function or activity that involves the creation, use, or disclosure of PHI. DHHS has offered some limited guidance on this topic, but significant gray area remains whether certain health care IT solutions require a Business Associate Contract.

A Business Associate Contract is not required between a covered entity and a health care IT solution provider if (1) the functions, activities, or services provided by the health care IT solution provider do not involve the use or disclosure of PHI and (2) where any access to PHI by such persons would be incidental. DHHS provided specific examples of vendors that would not be considered Business Associates -- janitorial services, electricians, and copy machine repair persons. Business Associate Contracts would not be necessary with these vendors because access to the PHI is not necessary for them to perform their jobs and any disclosure is limited in nature and occurs as a by-product of the vendor's duties.

DHHS has also stated that Business Associate Contracts are also not required where a vendor is merely acting as a "conduit" for PHI such as the US Postal Service, private couriers, and their electronic equivalents. A health care IT solution provider could be providing electronic transmission services for a covered entity and not be business

associate because the health care IT solution provider is merely a "conduit" analogous to the United States Post Office. In these situations, the determining factor is whether the health care IT solution provider can access the contents of the information it is transmitting for the covered entity. If the health care IT solution provider cannot access the information, a Business Associate Contract would probably not be necessary.

If a software vendor licenses electronic medical records software to a covered entity, that activity in and of itself probably does not require a Business Associate Contract. However, if the software vendor also performs some integration or customization where it will have access to PHI, a Business Associate Contract is probably required. If the software vendor's services include the use and disclosure of PHI or access to PHI will not be incidental because it is expected that the use and disclosure will occur, a Business Associate Contract should be in place. In the HIPAA context, incidental disclosure can be interpreted as a disclosure that is not anticipated when the relationship between the covered entity and the vendor is established.

Each health care IT solution provider will have to evaluate the specific circumstances of its relationship with the covered entity to determine whether a Business Associate Contract is required. Where it does not appear that a Business Associate Contract is necessary, the health care IT solution provider must be armed with sufficient rationale to convince the covered entity that a Business Associate Contract is not necessary. It may be possible to convince the covered entity to accept a modified Business Associate Contract in situations that fall into these gray areas, perhaps removing some of the covered entity's optional provisions that would create an additional burden on the health care IT solution provider.

Where the necessity of a Business Associate Contract is not clear-cut, the bargaining power of the covered entity may determine whether the health care IT solution provider enters into a Business Associate Contract. Some large software vendors have taken the position that any access they would have to PHI would be incidental and, therefore, a Business Associate Contract would not be necessary. For those covered entities that have an existing license agreement with a large software vendor, it may be impractical, if not impossible, to obtain a Business Associate Contract from such a vendor. On the other hand, smaller health care IT solution providers or health care IT solution providers that do not have an existing relationship with a covered entity may find it more difficult to avoid entering into Business Associate Contracts.

CRITICAL IMPLICATIONS

Once a health care IT solution provider enters into a Business Associate Contract, it must take the proper steps to comply with its business associate obligations. Upon entering into Business Associate Contracts, many health care IT solution providers simply put the contract in a file and forget about it. This approach may result from the suggestion by The Office for Civil Rights that "covered entities are not required to actively monitor or oversee the means by which the business associate carries out safeguards or the extent to which the business associate abides by the requirements of the contract." Moreover, many covered entities have been advised to avoid monitoring or evaluating their business associates' compliance with business associate obligations.

There is a growing trend towards covered entities evaluating their business associates' compliance with their business associate obligations. This trend is fostered by independent initiatives such as the JAHCO/NCQA Privacy Certification for Business Associates program and the potential for more aggressive enforcement of HIPAA by the Office for Civil Rights. In the JAHCO/NCQA Privacy Certification program, JAHCO/NCQA will certify a business associate as complying with certain Privacy Rule "standards." Business associates that obtain such certification from JAHCO/NCQA will inevitably use that certification as a marketing tool. As business associates began to market themselves as "certified" business associates to differentiate themselves from their competitors, there will be a strong impedes on covered entities to do some evaluation of potential and existing business associates. Soon the standard of care for covered entities will require some due diligence surrounding business associates' compliance with their business associate obligations. Last summer, the Health Privacy Project criticized the Center for Medicare & Medicaid Service's HIPAA enforcement plan that relies on a complaint based process and advocated routine monitoring of covered entities' HIPAA compliance. Part of that routine monitoring may evaluate the covered entities' relationships with their business associates.

With increased scrutiny of their compliance with their business associate obligations, health care IT solution providers must understand that a failure to comply with those obligations can result in a termination of their relationship with the covered entity or even a lawsuit for breach of contract. Situations have already occurred where a covered entity who wants to terminate a multi-year services agreement is contractually allowed to do so because its business associate is not complying with its business associate obligations.

Complying with Business Associate Obligations

For a health care IT solution provider that has entered into a Business Associate Contract with a covered entity, the ability to comply with business associate obligations can be complicated. The level of complexity increases by the number of Business Associate Contracts that the health care IT solution provider has entered into and the variation among the terms of the various Business Associate Contracts. For the lucky health care IT solution provider who is in a strong bargaining position vis-à-vis its customers, the health care IT solution provider may have a standard business associate agreement that it has all of its customers sign. For the vast majority of health care IT solution providers, they have signed a number of Business Associate Contracts with not only many of the standard terms but also many optional provisions.

To comply with its business associate obligations, a health care IT solution provider will need to develop internal policies and procedures for handling or gaining access to PHI. Those policies and procedures should track the requirements of the most onerous Business Associate Contract that the health care IT solution provider has entered into. In some instances, the health care IT solution provider may be in a position where it is maintaining PHI for the covered entity, such as an electronic medical records in an ASP environment. In such a situation, the health care IT solution provider may need to create an infrastructure and implement a system to allow patients to access and amend their PHI. In addition, the health care IT solution provider may need to create an

infrastructure and implement a system to provide an accounting of disclosures in accordance with the Privacy Rule.

A few of the standard provisions and some of the common optional provisions in a Business Associate Contract require special attention. One of the most difficult business associate obligations with which a health care IT solution provider must comply is the requirement that it ensure that its agents and subcontractors to whom it provides PHI agree to the same restrictions and conditions that apply to the health care IT solution provider with respect to the PHI. This is especially true when the health care IT solution provider utilizes a number of contractors or downstream providers that will come into contact with the PHI. The difficulty in complying with this provision is that most health care IT solution providers will have previously existing contractual relationships with these downstream vendors. The Business Associate Contract essentially asks these health care IT solution providers to go back to these downstream vendors and ask them to assume additional obligations. Some of these downstream vendors will resist or seek compensation to agree to such additional burdens.

Another provision that has created problems in Business Associate Contracts is the requirement that the Business Associate Contract must establish the permitted uses and disclosures of PHI by the business associate. Many Business Associate Contracts fail to specify the use of the PHI and the persons to whom further disclosures may be made. This deficiency usually occurs because covered entities draft standard form Business Associate Contracts and fail to take the time to adapt individual Business Associate Contracts to the unique services being provided by each health care IT solution provider.

What should a health care IT solution provider entering into Business Associate Contracts do as a result? It should specify for the covered entity the purposes for which it may use the PHI and the types of persons to whom the health care IT solution provider may make further disclosures. The health care IT solution provider is the only person in the relationship that can specify this information. If these parameters are not specified in the Business Associate Contract, an inherent ambiguity will be created causing potential disputes between the covered entity and the health care IT solution provider. In the very near future, covered entities will pay much more attention to this aspect of their Business Associate Contracts prompting, in many circumstances, amendments to existing Business Associate Contracts.

There also may be a number of optional provisions that the health care IT solution provider agrees to accept in the Business Associate Contract. The health care IT solution provider should ensure that it has taken proper steps to comply with any such obligations.

LIABILITY

HIPAA imposes harsh penalties for noncompliance. Although health care IT solution providers are not expressly subject to HIPAA, unless they are found to be “covered entities,” every health care IT solution provider must still be concerned about potential liability. This liability can arise under any number of scenarios.

Some covered entities may seek indemnification from a health care IT solution provider for any HIPAA violations that occur as a result of the health care IT solution provider's actions. However, a covered entity will probably not be held in violation of HIPAA based upon the actions of its business associates. As a result, the consequences of any such indemnification obligations should be minimal. A health care IT solution provider could agree to an indemnification provision for HIPAA violations that result from its actions, because there is little likelihood that the covered entity will be held responsible for the actions of its business associates. On the other hand, a health care IT solution provider could refuse to provide such indemnification on the basis that the covered entity cannot be subject to HIPAA fines for the action of its business associates.

One area of concern for health care IT solution providers should be civil lawsuits brought by aggressive plaintiffs' lawyers because of the increased awareness of health care privacy and security concerns. Prior to the effective date of the Privacy Rule, courts had ruled that the Privacy Rule was the standard in handling PHI. We expect similar rulings in connection with the Security Rule. Again, the covered entity may seek indemnification from its health care IT solution provider for situations where civil lawsuits are based upon an action that the health care IT solution provider did or did not take. The primary factor in assessing who has responsibility for resulting liability associated with a lapse by a health care IT solution provider is the contract between the health care IT solution provider and the covered entity. Deftly drafted contracts will be the key to allocating responsibility between health care IT solution providers and their customers.

An even more troubling concern for health care IT solution providers is potential criminal prosecution. It may be possible under certain situations for business associates to be prosecuted under HIPAA. If a health care IT solution provider agrees in its Business Associate Contract to comply with HIPAA, it could be deemed to be subject to HIPAA's requirements. HIPAA also does not expressly exclude entities other than clearinghouses, health plans, or providers from being subject to HIPAA so the term "person," which is used broadly in many sections of HIPAA, could be extended to cover not only covered entities, but also business associates. Also, as the range of solutions provided by health care IT solution providers expands into areas such as preventative health care, some health care IT solution providers could be deemed to be "covered entities" under HIPAA because they furnish, bill, or are paid for care, services, or supplies related to the health of an individual.

CONCLUSION

For success, a health care IT solution provider must address the developing concerns of its potential customer base. One such developing concern for customers of health care IT solution providers is HIPAA. Consequently, understanding and addressing HIPAA and its implications, both internally and for potential customers should be a central focus for health care IT solution providers.

About the paper

This White Paper is jointly published by and the Information Technology Association of America. The Rotbert Law Group, LLC focuses include information technology law, including HIPAA privacy and security. Some of its attorneys' accomplishments include negotiating a $500 million information technology and business process outsourcing transaction on behalf of a client with EDS and co-chairing an Information Technology Association of America committee that prepared and publicly released service level agreement guidelines for the health care sector.

The principle author John A. Bonello is an attorney with the Rotbert Law Group, LLC in Rockville Md. He provides counseling to businesses on a wide range of matters such as business formation, complex commercial transactions, licensing, privacy, outsourcing agreements, and e-business issues. Mr. Bonello spearheaded the creation of the ITAA's ASP Service Level Agreement Guidelines and is Co-Chair of ITAA's Sub-Committee that prepared the ITAA's ASP Service Level Agreement Guidelines for the Health Care Sector. For more information, please contact John Bonello (301)217-5910 or jbonello@rotbertlaw.net

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 400 corporate members throughout the U.S., and a global network of 53 countries' IT associations. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. For more information visit www.itaa.org.

ITAA's *E-Health Program* was established to engage in marketplace development and education in order encourage the healthcare community, information technology providers, employee groups, employers, payers, and government institutions to make better use of information technology resources. ITAA's "E-Health Success Story Webcast" series provides concrete ideas about using information technology (IT) to improve healthcare. For more information contact Mark Uncapher, ITAA Senior Vice President & Counsel at muncapher@itaa.org.