



James River Consulting

Better IT & Services Contracting

www.jamesriverllc.com

A professional services firm specializing in IT and business services contracts, outsourcing, on demand, e-contracting, contracts processes, and contracts management staffing

# Newsletter

Q4 2010

TO RECEIVE BY EMAIL PLEASE REPLY TO [info@jamesriverllc.com](mailto:info@jamesriverllc.com) WITH "EMAIL NEWSLETTER" IN THE SUBJECT LINE

## Feature Article

### HIPAA Business Associate Agreements

In the Q2 2010 Newsletter we discussed how the EU Privacy Directive and the Massachusetts comprehensive information security program (CISP) law extended the coverage of those laws to include suppliers and business partners, by requiring the companies who collect the data to use prescribed terms in their contracts with the partners and suppliers, even though the third party companies at the other end of the contracts may never have expected, or wanted, or possessed the capability to take on the associated costs and the liabilities. The point of the Q2 article was the phenomenon of governments applying laws via contract terms, what you might call "regulation by contract." Regulation by contract is something more than the terms often seen in business contracts requiring one party to comply with laws aimed at the other party in a vertical industry, e.g., FDA, or comply with laws that the other party feels to be socially responsible, e.g., EEOC. With regulation by contract, contract terms are mandated by the law as a means of extending the reach of the law to achieve greater efficacy.

A third example of regulation by contract is HIPAA, the Health Information Portability and Accountability Act, and its recent amendment by HITECH (Health Information Technology for Economic and Clinical Health Act). HIPAA was passed in 1996 and first went into effect in 2001. In a nutshell, the law limits what hospitals and doctors' offices are permitted to do with patient information and the uses (research, marketing) for which they need patient consent (Privacy Rule); what safeguards they must follow to protect the confidentiality, integrity and availability of the data (Security Rule); and when health care providers must notify patients of breaches of data systems (Breach Notification Rule).

Most sales and project people know about HIPAA through a particular kind of contract called the business associate agreement or BAA. BAAs appear both in the form of addendums to services contracts and as standalone agreements

meant to amend existing contracts or to cover overall business dealings. Anyone who has dealt with BAAs knows that they are a negotiation in and of themselves and often prove more difficult than the vendor's services agreement. For reasons that we will see below, BAA negotiations are especially painful. Failure to come to agreement over a BAA will certainly kill any deal in the healthcare industry.

As Richmond based Hunton and Williams lawyer Mark Hedberg points out in the December, 2009, issue of the ABA's Health eSource newsletter, the shocking truth about BAAs is that they were never part of the original HIPAA statute. It was the Department of Health and Human Services (HHS) that, recognizing the regulatory hole left by the law's failure to address healthcare suppliers and partners, created BAAs in the regulations (45 CFR 160, 164) implementing HIPAA.

BAAs must spell out what are and are not permissible uses of patient information according to the regulations. BAAs must specify that business associates will employ security safeguards for electronic patient information. BAAs must authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. Under BAAs, business associates are obligated to make available data for rendering an accounting of all disclosures upon patient request. And BAAs must outline the handling of patient information upon termination of the services contract.

Then came HITECH in 2009. Congress expanded HHS's jurisdiction to include 3<sup>rd</sup> party suppliers and business partners to healthcare providers, both by adopting a very broad definition of what makes a company a business associate, and by imposing on business associates the same civil and criminal penalties for HIPAA violations that apply to healthcare companies. The final regulations implementing HITECH's new business associate rules are still in the works.

*(Continued on other side)*



### About James River

James River Consulting specializes in the development, negotiation, and management of IT and business services contracts with emphasis on IT and business outsourcing and on software-as-a-service/cloud computing/managed services. James River's offerings range from short-term staffing of contracts personnel, to sales contract processes, to e-Contracts, to competitive bidding, to SaaS and BPO contracts negotiation and management. James River's president, Eric Esperne, has over 15 years experience as an in-house legal counsel and director of contracts for both large and small IT companies.

Copyright James River Consulting LLC

8 Goldenrod Drive, Medway, MA 02053 703.850.7061-Mobile  
[eesperne@jamesriverllc.com](mailto:eesperne@jamesriverllc.com) [jamesriverconsulting@comcast.net](http://jamesriverconsulting@comcast.net)

## Feature Article continued

Hedberg points out that this new approach might lead one to conclude that, by making business associates equally liable for HIPAA violations, Congress was also doing away with BAAs. Compared to direct regulation, BAAs are indirect and disruptive of the natural flow of commerce. To the contrary: Congress not only kept BAAs, but added to them. BAAs must now specifically require business associates to implement and maintain network security and other computer system safeguards when processing patient data in compliance with the regulations and HHS guidance. Further, HITECH mandates use of BAAs at the business associate -subcontractor tier where the subcontractor creates, receives, maintains or transmits patient data.

Much confusion reigns over BAAs. Some hospitals take the approach that BAAs require suppliers and partners to comply with HIPAA/HITECH requirements to the same extent as the hospitals, in effect step into the hospitals' shoes. Many healthcare provider-written BAAs ask vendors and partners to indemnify the hospital for penalties levied by the HHS Office for Civil Rights. 3<sup>rd</sup> party service providers to hospitals have their own take on BAAs. What most service providers are concerned about are transaction related compliance costs; these costs are especially unwanted when the service provider is not really in a line of business that profits from the content of patient information, such as remote information management. Nor do service providers want to end up becoming de facto HIPAA compliance consultants for free.

When the government requires parties to write their contracts in a certain way, the parties are forced to allocate risk in a certain way and not necessarily the most efficient or effective way. That's what transaction cost economics is all about, allowing businesses to set the rules. In the healthcare industry, service providers are now faced with little choice but to take on huge potential liability for data breaches and failure to implement adequate safeguards, even when the price tag for a job is only a few grand. Risk is linked to price in contracts. Either healthcare service providers will raise prices to cover the added risk; or service providers limit their scope of work and force hospitals to in source much of their IT and business operations; or providers will bite the bullet, become expert at HIPAA compliance, and implement the administrative, physical and technical safeguards.

Here are a few guidelines for service providers to follow in dealing with BAAs:

- Accept that you are a business associate
- Accept that if the customer has their own BAA they will insist you use theirs
- The HHS regulations are your baseline for reviewing BAAs
- Review the BAA from two angles, costs and risks
- Address costs on a strict "bring your own" basis
- Address risk through carefully drafting the statement of work
- Don't mash up HIPAA with confidentiality and state data security laws

For more, contact Eric Esperne, President at 703-850-7061 or email him at [eesperne@jamesriverllc.com](mailto:eesperne@jamesriverllc.com).

## Company News

**Dell Services** Eric Esperne, President of James River Consulting, has taken a position with Dell Services, a business unit within Dell Inc. focusing on systems implementation, managed services, and professional IT and business consulting. Eric will continue to provide services as a consultant, subject to any potential conflict of interest or other limitations per agreement with Dell.

**Presentations** On October 21, Eric Esperne was the featured expert on the IACCM's Ask the Expert audio conference call, speaking on risk management in contracting to a worldwide audience. Eric is now being regularly contacted by NCMA chapters, ISM chapters and other organizations interested in risk management.



8 Goldenrod Drive, Medway, MA 02053

# Newsletter