

message from partner in charge

As we look back on the second quarter, Mr. Adler and I report on the new HITECH Act, which focuses on developing a nationwide health information technology infrastructure that supports electronic health records and health information exchanges.

In an online seminar, Ms. Demont, Mr. London and Mr. Rosener will participate in a August 5 webinar addressing recent trends in shareholder activism and reasons why directors and management should be proactive.

We report that merger and acquisition activity is likely to increase during the remainder of the year as a result of the high level of distressed debt, according to a study commissioned by Carl Marks Advisory Group LLC and Pepper. Pepper also will host a webinar on this topic; see page 5 for details.

In Pepper's world online, Mr. Canavan is featured in a Peppercast to help employers plan layoffs to consider the morale of those remaining employed.

Sharon R. Klein
949.567.3506
kleins@pepperlaw.com

in this issue

- 1 **HITECH Act Aims to Create Nationwide Health Information Technology Infrastructure while Protecting Patient Privacy and Security**
- 2 **Peppercast: Reductions in Force - What About Those Left Behind?**
- 3 **Addressing Recent Trends in Shareholder Activism: Directors and Management Should be Proactive**
- 5 **Market Conditions to Produce Significant Distressed M&A Opportunities in Second Half of 2009**
- 5 **Distressed M&A Outlook Webinar**

HITECH Act Aims to Create Nationwide Health Information Technology Infrastructure while Protecting Patient Privacy and Security

A version of this article appeared in the May 11-17, 2009 issue of Orange County Business Journal. It is reprinted here with permission.

The American Recovery and Reinvestment Act of 2009 (ARRA), effective on February 17, 2009, includes the Health Information Technology for Economic and Clinical Health (HITECH) Act, which focuses on developing a nationwide health information technology (HIT) infrastructure that supports electronic health records and health information exchanges. To accomplish this, the act provides for:

- creating standards, implementation specifications and certification criteria for network interoperability, and
- implementing the health network and electronic health records (EHRs) through grants, loan funds, incentive programs, and information sharing.

The HITECH Act, recognizing that the successful adoption of HIT relies on privacy and security, includes provisions intended to enhance and strengthen the privacy and security of health information as it is received, created, processed, stored and transmitted over the nationwide HIT infrastructure. In this article, we focus on the act's privacy and security provisions, which include:

- clarification and expansion of the definition of a "business associate"
- increased business associate legal obligations
- enhancement of enforcement, funding for enforcement and increased penalties
- notification for breaches involving protected health information (PHI), and

- special provisions for vendors of personal health records and other non-HIPAA covered entities.

Redefining a ‘Business Associate,’ and Their Increased Legal Obligations

The HITECH Act includes as business associates entities that provide data transmission services to a covered entity (or its business associate) if the service routinely involves access to PHI. This includes, for example, a health information exchange organization, a regional health information organization, an e-prescribing gateway, or any vendor that contracts with the covered entity to allow the entity to offer a personal health record (PHR) to patients.

Enhancing the Business Associate’s Legal Obligations

The HITECH Act provides that each administrative, technical and physical security and privacy requirement in HIPAA that applies to a covered entity also directly applies to a business associate. A business associate must prepare and implement policies and procedures, and train employees as required by the security rule. These changes will enhance the business associate’s information security practices, and better enable a covered entity to monitor a business associate’s information security program.

The act provides that business associates that violate HIPAA’s security and privacy provisions are subject to the same civil and criminal penalties as a covered entity.

Enforcement of the Act and Penalties

Unlike the primarily voluntary compliance efforts to enforce HIPAA, the HITECH Act contains provisions intended to add teeth to ensure compliance with the enhanced privacy and security initiatives. Audits by the U.S. Department of Health and Human Services (HHS), heightened penalties and enforcement by states’ attorneys general indicate that the current administration means to take violations of privacy and security seriously.

Criminal and civil penalties extend to individuals as well as entities responsible for breaches. Criminal penalties for disclosing PHI include:

- for a basic knowing violation, a \$50,000 fine, imprisonment for not more than one year, or both
- with false pretenses, a fine of not more than \$100,000, imprisonment for not more than five years, or both, and
- with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, a fine of not more than \$250,000, imprisonment for not more than 10 years, or both.

Civil penalties with increasing monetary penalties with higher tiers based on willful intent have strengthened HIPAA sanctions. Civil penalties escalate to \$50,000 per violation and cap out at \$1.5 million per year. Funds collected will be channeled back to HHS to be used toward further enforcement. The government is investigating



Peppercast: Reductions in Force - What About Those Left Behind?

In this tough economy, many organizations have come to the conclusion that layoffs are necessary if the business is to remain afloat. Most companies try to come up with a plan for discharging those employees in a manner that maximizes their human dignity and minimizes disruption to your business operations.

In this podcast, Mike Canavan, an attorney in Pepper’s Princeton office concentrating his practice in labor and employment law, discusses how to get the most out of your remaining employees who are about to watch their friends and colleagues lose their jobs.

Listen today by visiting the Labor and Employment section of Pepper’s podcenter at www.pepperpodcasts.com.

whether a percentage of the penalties should be distributed to the victims of the security breach.

Enforcement by States' Attorneys General

A state's attorney general may bring a civil action on behalf of residents of a state in a U.S. District Court. Damages will be statutorily imposed:

- The amount is calculated by multiplying the number of violations by up to \$100.
- The total amount of damages imposed on the person for multiple violations of an identical requirement or prohibition during a calendar year shall not exceed \$25,000.
- Reasonable costs for bringing the action and attorney's fees may be awarded.

Notifications for Breaches Involving Protected Health Information

The HITECH Act adds federal notice of breach provisions similar to those in place in California and other states. It applies to business associates and covered entities that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI. A "breach of security" is an acquisition, access, use or disclosure of unsecured (i.e., unencrypted) PHI. Remember that breaches occur not only when data is unencrypted in transit or storage but when PHI is not completely erased or destroyed.

The act requires any encryption technology used to be developed or endorsed by a standards developing organization accredited by the American National Standards Institute, or otherwise through the use of technology or methodology specified by the secretary of HHS. Proposed guidance on breach notification was issued by HHS on April 17, 2009 for comment.

- *Breaches Experienced by a Covered Entity*

Following the discovery of a breach, a covered entity shall notify each individual whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired or disclosed as a result of the breach. Notice must include a brief description of what happened and when, and an accounting of the PHI that was compromised, what individuals must do to protect themselves, and how the covered entity responded to the breach. Also required are identification of the

Addressing Recent Trends In Shareholder Activism: Directors and Management Should be Proactive

August 5, 2009

12:00 – 1:00 P.M. EASTERN

Join us for a complimentary, one-hour online seminar that will focus on the trends in shareholder activism, recent developments in Delaware corporate law, the SEC's proposed regulations on proxy access, the current status of poison pills and recommended actions for directors and management.

Speakers

Valérie Demont, Partner, Pepper Hamilton LLP
Richard De Rose, Managing Director,
Houlihan Lokey

Steven R. London, Partner, Pepper Hamilton LLP
James D. Rosener, Partner, Pepper Hamilton LLP

Register online at

https://www.regonline.com/Shareholder_Activism or contact Brian Dolan at dolanb@pepperlaw.com.

covered entities, their contact information, and ways people can get further information about the breach from the covered entities.

A covered entity or a business associate (including any employee, officer, or other agent of the entity or associate other than the individual committing the breach) should consider a breach "discovered" on the day they first know of it, or reasonably should have known it had occurred. Unless delayed for law enforcement purposes, notifications must be prompt, never later than 60 days after the breach is discovered.

Notice may be written and sent by mail or e-mail. If mailing or e-mail addresses are unavailable or insufficient, substitute notice may be provided by placing a conspicuous posting on the home page of the covered entity's Web site or via major print or broadcast media. Substitute notice must include a

toll-free number that people can call to learn whether their unsecured PHI is included in the breach. Notice also may be provided to the media if the breach of PHI involves more than 500 people.

Breaches involving more than 500 people must be reported immediately to HHS, which will post on its Web site a list of covered entities involved in breaches of more than 500 people, and shall provide annual reports of breaches to Congress.

- *Breaches Experienced by a Business Associate*

A business associate must notify the covered entity following the discovery of a breach. The notice must identify each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during the breach.

- *Breaches Involving Vendors of Personal Health Records and Other Non-HIPAA Covered Entities*

Additional provisions for notice of breaches apply to PHR-related entities, which are: (i) vendors of PHRs, (ii) entities that offer products or services through the Web site of a vendor of PHRs, (iii) entities that are not covered entities and that offer products or services through the Web site of covered entities that offer individuals' personal health records, and (iv) entities that are not covered entities that access information in PHRs or send information to a PHR.

The PHR-related entity also must notify the Federal Trade Commission, which in turn will notify HHS of the breach. A violation of the breach requirements will be treated as an unfair and deceptive act or practice in violation of the regulations under the Federal Trade Commission Act, and will be enforced as such.

The requirements for timing, method and content of notifications are the same as those applying to covered entities. Similarly, PHR identifiable health information is unsecured when it is not encrypted.

The notice provisions also apply to a third-party service provider that handles PHR identifiable health information on behalf of a PHR-related entity. The service provider must notify the PHR-related entity following discovery of the breach and identify each individual whose unsecured PHR identifiable health

The HITECH Act provides that each administrative, technical and physical security and privacy requirement in HIPAA that applies to a covered entity also directly applies to a business associate.

information has been (or is reasonably believed to have been) accessed, acquired or disclosed during the breach.

Conclusion

The HITECH Act imposes new privacy and security requirements that affect many covered entities, business associates and non-HIPAA covered entities, which all need to understand and analyze how the provisions affect them, and act on any deficiencies. It is important to scrutinize your use of data and de-identify PHI as much as possible so that you are not subject to regulation. To the extent that de-identification of PHI is not possible, here are some compliance steps you might consider: All affected organizations should conduct mini-assessments of the legal compliance of their information security and privacy practices and integrate any needed changes into their current compliance program. New business associates need to develop standard operating procedures, to train employees and to understand their compliance obligations. All covered entities and business associates must study the new federal security breach provisions. They should form an interdisciplinary SWAT team ready to respond to any breach, have forms of breach notice ready, and understand to whom and when such notices must be provided. Regulations and guidance will be forthcoming—keep abreast of them and take advantage of the comment periods. The first guidance on breach notifications hopefully will shed light on whether limited data sets (like those used for research, which de-identify some data fields but need others to remain for the integrity of the research study) are subject to the same breach regulations. Also, the guidance assists in understanding encryption rules and harmonizing the federal and state breach notification provisions.

A full version of this article can be viewed online at
http://www.pepperlaw.com/publications_update.aspx?ArticleKey=1416.

Authors:

M. Peter Adler
202.220.1278
adlerp@pepperlaw.com

Sharon R. Klein
949.567.3506
215.981.4172
kleins@pepperlaw.com

Distressed M&A Outlook Webinar

August 11, 2009
12:00 – 1:00 P.M. EASTERN

To gain perspective on the current distressed M&A market, Carl Marks Advisory Group LLC and Pepper Hamilton LLP commissioned mergermarket, a research and publishing company, to survey a diverse group of corporate executives, private equity practitioners, hedge fund investors and lawyers regarding the foremost issues facing distressed investors today.

Join us for a complimentary, one-hour online seminar, that will discuss the report findings and implications for the combination of eager sellers and opportunistic buyers who will undoubtedly provide fuel for distressed activities in the second half of 2009.

Register online at https://www.regonline.com/Distressed_MA_Opportunities.

Please contact Brian Dolan at dolanb@pepperlaw.com with questions about the event or to request a copy of the study.

Market Conditions to Produce Significant Distressed M&A Opportunities in Second Half of 2009

The current economic downturn will offer greater discounts on distressed assets than previous downturns have offered, drawing both financial and strategic buyers to the market in the coming months, according to 92 percent of respondents to a new **Distressed M&A Outlook** survey conducted by mergermarket, Carl Marks Advisory Group LLP and Pepper Hamilton LLP.

In the second quarter of 2009, Carl Marks Advisory Group LLP and Pepper Hamilton LLP commissioned mergermarket to survey 75 investment bankers, private equity practitioners, hedge fund investors and lawyers regarding their outlook for distressed M&A activity in the upcoming year. Respondents provided invaluable insight into current market conditions, as well as a forecast for the year ahead.

“With a variety of factors contributing to an increased volume of distressed opportunities, both buyers and sellers are expected to eagerly pursue deals, as each side stands to gain unique benefits,” said Jim Rosener, managing partner of the New York office and head of the International Practice Group at Pepper Hamilton LLP.

Aside from attractive discounts, debt-related issues will likely be the most prominent drivers of distressed M&A activity in the upcoming year, according to respondents. An increase in covenant defaults is identified as a major catalyst to distressed deal flow, as is companies’ inability to meet debt obligations or refinance upcoming maturities.

Distressed investors are likely to find the greatest opportunity in the following two sectors:

- Real Estate, where 63 percent of respondents expect to see the highest volume of distressed deals in the year ahead, and
- Financial Services, which 38 percent of respondents believe will experience the highest volume of distressed M&A this year.

63 percent of respondents expect most distressed deals to be handled outside of court; however, Chapter 11 reorganizations may be an exception as these are expected to be extremely common over the next 12 months.

The predominance of out-of-court deals is likely related to time constraints, as many respondents cite time as a major drawback to handling deals in court. 59 percent of respondents say the distressed M&A process can exceed four months when handled in court. Meanwhile, on cases handled outside of court, only 25 percent of respondents say the process can take this long. “If implementable, out-of-court solutions are generally less expensive and disruptive. However, it is not clear whether companies with complex capital structures will ultimately be able to obtain all of the consents necessary to use these solutions,” explains Duff Meyercord, partner at Carl Marks.

Time constraints also are expected to put pressure on management teams within distressed companies, which in turn may influence the dynamics of distressed transactions going forward. According to Jim Rosener, “Not only is the market characterized by people having to do something and forced to do it on a tight timetable, but there also is an increased opportunity as management loses focus and interest over these orphaned businesses.”

Additional findings:

Exit outlook: 65 percent of respondents plan to delay their exits from distressed investments in the upcoming year.

Valuations: 54 percent of respondents say asset-based valuations tend to be the primary determinant of price.

Alternative strategies: 79 percent of respondents expect debt buy-backs to increase in the year ahead.

If you would like a copy of this report, please contact Brian Dolan at 215.981.4568 or dolanb@pepperlaw.com.

Pepper Hamilton LLP

Attorneys at Law

The material in this publication is based on laws, court decisions, administrative rulings and congressional materials, and should not be construed as legal advice or legal opinions on specific facts.

The information in this publication is not intended to create, and the transmission and receipt of it does not constitute, a lawyer-client relationship.

Please send address corrections to phinfo@pepperlaw.com.

www.pepperlaw.com

Berwyn | Boston | Detroit | Harrisburg | New York | Orange County
Philadelphia | Pittsburgh | Princeton | Washington, D.C. | Wilmington

© 2009 Pepper Hamilton LLP. All Rights Reserved.

This publication may contain attorney advertising.