

Corporate Communiqué

In this issue

*Stimulus Act and Newly
Adopted Regulations Affect
Many Members of the Health
Care Industry*

Page 1

*Social Media Sites Raise New
Questions for Employers*

Page 3

*Rothman Gordon Accepted to
Primerus, an International Law
Consortium*

Page 4



Rothman Gordon, P.C.
Attorneys At Law
310 Grant Street
Third Floor, Grant Building
Pittsburgh, PA 15219
(phone) 412.338.1100
(fax) 412.281.7304
www.rothmangordon.com

© 2009 Rothman Gordon, P.C.

The contents of this newsletter are intended for general information purposes only, and should not be relied upon as a substitute for obtaining legal advice applicable to your situation.

Stimulus Act and Newly Adopted Regulations

Affect Many Members of the Health Care Industry

By Bernadette L. Puzzuole, Esq. and Chad D. Tomosovich, Esq.

We have all read or heard stories about someone improperly accessing the medical records of a celebrity, and then selling that information to the media (e.g., National Enquirer). The Health Insurance Portability and Accountability Act ("HIPAA") has, for years, imposed obligations on medical providers to prevent such unauthorized disclosure of information they control. Under one section of the American Recovery and Reinvestment Act of 2009 (the "Stimulus Act"), these HIPAA security obligations have been extended beyond medical providers (i.e. Covered Entities), and now affect businesses and individuals that provide support services to medical providers (i.e. Business Associates). If your business is either a "Covered Entity" or "Business Associate", the time to become familiar with these provisions of the Stimulus Act is now, because some of these obligations became effective September 23, 2009, and others will become effective February 17, 2010.

In order to understand the provisions of the Stimulus Act, you must become familiar with certain basic terms defined by HIPAA. Protected Health Information is health information by which a particular individual can be identified, and which is transmitted or maintained in electronic media, paper or other form. Protected Health Information includes not only patients' names, addresses and health conditions, but also their social security numbers, billing information (including credit card information), and birth dates. Unsecured Protected Health Information is Protected Health Information that is not encrypted or, if being destroyed, is not destroyed in a specified way to prevent reconstruction. A Covered Entity is a business that transmits Protected Health Information in electronic form. Hospitals, health plans, billing services, physicians, medical practices, and all of their employees are examples of Covered Entities. A Business Associate is a person or entity that is not an employee of a Covered Entity, but performs tasks for the Covered Entity or assists the Covered Entity in some of its activities, and as a result has access to Protected Health Information. Claims processors, practice management services, and data processing personnel are all examples of Business Associates.

With these terms in mind, the portion of the Stimulus Act imposing these new security obligations is the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). The main focus of the HITECH Act is to establish financial incentives for Covered Entities to convert their Protected Health Information to a form of electronic media. Because the unauthorized disclosure of Unsecured Protected Health Information poses significant risks, the HITECH Act also imposes significant security obligations on Business Associates to prevent such disclosure, and imposes

Continued on page 2

notification obligations on Business Associates and Covered Entities if unauthorized disclosure occurs.

SECURITY REQUIREMENTS. Covered Entities have, for many years under HIPAA, been required to implement security plans and procedures to prevent unauthorized disclosure of Unsecured Protected Health Information. Under the HITECH Act, Business Associates must, by February 17, 2010, implement those same or similar security plans and procedures. The components of those security plans are quite detailed and strict compliance is required. Civil and criminal penalties can be imposed for non-compliance.

NOTIFICATION REQUIREMENTS. In addition to imposing security obligations on Business Associates, the HITECH Act also imposes new notification requirements on both Business Associates and Covered Entities whenever Unsecured Protected Health Information is disclosed to unauthorized personnel. In some cases the notification of the unauthorized disclosure must be directly to the person whose Unsecured Protected Health Information was disclosed, and in other cases, the media must also be notified of the unauthorized disclosure. The Secretary of the Department of Health and Human Services (“Secretary”) must be notified of each unauthorized disclosure, with the timing of the notice dependent on the number of individuals involved. Business Associates are required to notify a Covered Entity about unauthorized disclosure of Unsecured Protected Health Information of that Covered Entity which occurs at the Business Associate level. Covered Entities are required to notify the Secretary, individuals and/or media of the unauthorized disclosure, whether at the Covered Entity or Business Associate level. The HITECH Act details the methods by which individuals must be notified and imposes strict timelines for this notification. Civil and criminal penalties can be imposed for non-compliance.

ISSUES TO CONSIDER. If you are a Covered Entity or Business Associate there are several things you should consider:

BUSINESS ASSOCIATES

- Develop a security plan and procedures to bring your operations into compliance with the HITECH Act;
- Establish a procedure for discovering and providing notice to Covered Entities of any unauthorized disclosure of Unsecured Protected Health

Information in your control;

- Develop and implement procedures to reduce the amount of Unsecured Protected Health Information maintained; and
- Look for business opportunities with Covered Entities who may no longer wish to engage Business Associates located outside the United States.

COVERED ENTITIES

- Review and revise, as required, contracts with Business Associates to confirm their compliance with the security requirements of the HITECH Act and protect you for their noncompliance;
- Revise contracts with Business Associates to confirm their notification obligations under the HITECH Act and to provide protection for their noncompliance;
- Establish procedures to monitor compliance by Business Associates with the HITECH Act;
- Specify responsibility in contracts with Business Associates for the costs of notification, fines, penalties and remediation under the HITECH Act for unauthorized disclosures at the Business Associate level;
- Develop and implement procedures to reduce the amount of Unsecured Protected Health Information maintained;
- Establish procedures for discovering and providing notice of unauthorized disclosure of Unsecured Protected Health Information; and
- Look for business opportunities with other Covered Entities who may no longer wish to engage Covered Entities located outside the United States (e.g., billing service).



Chad Tomosovich is an attorney in the Corporate Department and head of the Health Care & Physician Practice Group. Chad can be reached at (412) 338-1119 or cdtomosovich@rothmangordon.com.



Bernadette Puzzuole is an attorney in the Real Estate and Corporate Departments and a member of the Health Care & Physician Practice Group. Bernie can be reached at (412) 338-1129 or bpuzzuole@rothmangordon.com.

Social Media Sites Raise New Questions for Employers

By Cami L. Davis, Esq.

Many companies have been trying to figure out how to harness the power of social media to generate business. Sites such as Twitter, Linked In, Facebook or personal blogs can be a terrific way to engage new customers, create buzz, and tell the story of your business.

The flip side is employers are not the only ones using social media. Employees are too. It's natural for employees to talk about where they work and it's natural that they may sometimes complain about their job or their supervisors. However, while this type of venting was once relegated to casual talk at the bar or among friends, social media introduces a whole new layer of concern for employers. The first issue is accessibility. Derogatory comments repeated among employees in a social situation generally won't travel much further. But those same comments repeated in a virtual social situation can suddenly be seen by thousands, if not millions, of people.

The natural urge is to curb employees' use of social media to protect your company's reputation or proprietary information. However, in doing so, you may be unintentionally creating liability on several fronts. And as social media is a relatively new medium, there is little case law to direct employers' actions.

A large part of the debate is what is private versus what is public. If an employee posts something defamatory on a public site, then the employee is taking the chance his or her employer might see and react. However, if the employee posts something on a private site (i.e. Facebook) and the employer uses improper means to view the posting, then the employer is taking a chance of violating the Federal Stored Communications Act. For example, in *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*, two employees were fired after posting sexual remarks about managers and customers on a password protected MySpace account. The employer gained access to the site through a third employee who gave the employer her password. If the third employee perceived that she would lose her job if she did not comply, then the labor laws would have been violated. In *Pietrylo*, the jury found that the third employee was impermissibly pressured into giving her password, thus violating the Stored Communication Act.

Some companies have reacted by banning use of social media by their employees. While an employer is

within its rights to ban use of social media on company time, it cannot dictate what employees do on their own time. Furthermore, overly broad social media policies could run afoul of employees' rights to have legitimate conversations regarding workplace conditions, terms, salaries and benefits as protected under Section 7 of the National Labor Relations Act, which protects employees' right to organize and bargain collectively.

An employer may also be setting itself up for future litigation. Should an employer discover protected information about an employee (such as disability or sexual orientation) and the employee is later terminated, a jury could view the termination as discriminatory.

Employers can terminate employees for defamatory statements published electronically, but how that information is acquired must be legal. Rothman Gordon strongly advises its corporate clients to incorporate social media policies into its current employee handbook and/or guidelines that are specific as to what is and is not acceptable.



Cami Davis is an associate with Rothman Gordon in the Labor and Employment Law and Employment Litigation Departments. While Cami concentrates her practice on litigation, she works with clients on a variety of issues, including counseling related to employment policies and practices, employment discrimination, employment agreements, wage and hour issues, unemployment compensation and other human resource matters. Cami can be reached at (412) 338-1127 or clDavis@rothmangordon.com.

Doug DeNardo recently joined Mark Lumley, VP, Trust Administration for NexTier Wealth Management for a podcast on *Choosing Beneficiaries: Opportunities, Pitfalls and Fact vs. Fiction*. You can access the podcast via the Rothman Gordon homepage or at www.thebank.com/B801.php.



Rothman Gordon Accepted to Primerus, an International Law Consortium

Managing Shareholder Bill Lestitian recently announced that Rothman Gordon has joined the Primerus International Law Consortium. Primerus is an international network of top-rated, independent mid-sized law firms. Candidates for membership must have the maximum AV rating from Martindale-Hubbell and submit to a rigorous evaluation which includes candid assessments from judges, fellow attorneys, current and former clients, bar associations, and malpractice insurance carriers. Firms must also attest to their commitment to the exacting standards of the Six Pillars of Primerus Quality: Integrity, Excellent Work Product, Reasonable Fees, Continuing Legal Education, Civility, and Community Service.

"We believe our affiliation with Primerus will enable us to better serve our clients. We are now linked to top rated mid-sized firms across the country, which

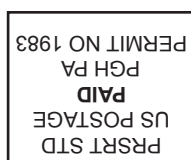
means we can connect our clients with law firms in multiple jurisdictions," says Managing Shareholder Bill Lestitian.

"A good way to pick the good (lawyers) from the bad, a sort of Good Housekeeping seal of approval."

--The Wall Street Journal

"The Primerus membership allows us to expand our goal to be "just right". The network we have entered will enable us to provide our clients with resources across the country, and even internationally, at reasonable fees," says Marketing Director Anne Parys.

Primerus law firms are located in over 115 cities throughout the United States, Canada, and the United Kingdom and offer expertise in hundreds of practice areas. Bill Lestitian, Bob Galanter and Chad Tomosovich attended the annual conference of Primerus members in October, giving the firm valuable face time with our new colleagues.



Rothman Gordon P.C.
 310 Grant Street
 Third Floor, Grant Building
 Pittsburgh, PA 15219

**ROTHMAN
 GORDON**