HEALTHCARE**LEGAL**NEWS

June 21, 2012 • Volume 2, Number 5

IN THIS ISSUE

Self-Insurance Sham?

Healthcare Information Technology News

If The Office Of Civil Rights Doesn't Get You, The FTC Will : The FTC Charges a Debt Collection Firm and an Auto Dealership with Data Privacy Violations for Exposing Private Information through Peer-to-Peer File Sharing Networks

To Be BYOD Or Not To Be BYOD: Is A "Bring Your Own Device" Policy Right For Your Organization?

DW HEALTHCARE TEAM - NEWS & SUCCESS STORIES

Out Now
Brian Balow authored the *Allocation and Mitigation of Risk* chapter in the BNA E-Health Treatise, E-HEALTH, PRIVACY, AND SECURITY LAW, 2nd Ed. (Dec. 2011)

Ralph Levy, Jr. wrote *Beware the Bundle: Medicare Announces Pilot Program for Bundled Payments to Providers*, which appeared in Journal of Health Care Compliance, May - June 2012.

Tatiana Melnik wrote *Class Actions, Federal Actions, and State Actions: The Data Breach Saga Continues*, which also appeared in Journal of Health Care Compliance, May - June 2012.

On **June 28, 2012**, Brian and Tatiana will be speaking on the legal issues surrounding mobile health at the Health IT Innovation Summit – mHealth in California. You can learn more about the event here: http://www.weyond.com/himss/socal/hitis/2012/

SELF-INSURANCE SHAM?

By Cynthia A. Moore, a member in Dickinson Wright's Troy office, can be reached at 248.433.7295 or cmoore@dickinsonwright.com

One way that employers seek to control health plan costs is by self-insuring the plan. By self-insuring, an employer pays only the cost of claims plus an administrative fee to a third party administrator. An employer can insure against the risk of catastrophic claims by purchasing stop loss insurance. An added benefit is that self-insured plans are exempt from most State insurance laws, such as laws mandating that certain benefits be covered. This gives an employer with a self-insured plan more flexibility to design the health plan to control costs and meet the needs of its employees. Although traditionally only large employers have self-insured their health plans, news reports indicate that more small employers may be considering the self-funding alternative.

On May 1, 2012, the Departments of Labor, Treasury, and Health and Human Services issued a Request for Information Regarding Stop Loss Insurance, in which the Departments asked a series of questions about stop loss insurance for health insurance plans. Stop loss insurance allows an employer to self-insure for a fixed amount of claims,

with stop loss insurance covering the remainder of the clams that exceed the fixed amount, called the "attachment point."

Under the principles of ERISA preemption, employers and health plans that purchase stop loss insurance generally are not subject to State insurance laws including mandated benefit laws, rating policies, and other State and Federal consumer protections applicable to health insurance, including some of the patient protections under the Patient Protection and Affordable Care Act ("Affordable Care Act"). Some experts have suggested that certain small employers (particularly those with healthy employee populations) may choose to self-insure and purchase stop loss insurance policies with relatively low attachment points to avoid being subject to these requirements while exposing themselves to little risk. For example, if the attachment point were set at $5,000 per employee or $100,000 for a group, a small employer would be assuming a low degree of risk and yet exempting itself from State insurance regulation. If a large number of employers were to follow this path, it could worsen the risk pool and increase premiums in the fully insured small group market, including in the Small Business Health Options Program (SHOP) Exchanges that will be available on January 1, 2014. In other words, adverse selection could threaten the financial stability and ongoing viability of the small group market and the SHOP Exchange.

According to the Request for Information, the Departments have little data on the incidence or terms of stop loss insurance among self-insured employer group health plans, and are soliciting comments (due by July 2, 2012) that will contribute to the Departments' understanding of the current and emerging market for stop loss products. After reviewing the comments, further regulations could be issued if the Departments determine that a trend toward self-insuring by small employers could threaten the small group market and/or the SHOP Exchange.

HEALTHCARE INFORMATION TECHNOLOGY NEWS

IF THE OFFICE OF CIVIL RIGHTS DOESN'T GET YOU, THE FTC WILL

The FTC Charges a Debt Collection Firm and an Auto Dealership with Data Privacy Violations for Exposing Private Information through Peer-to-Peer File Sharing Networks

By Tatiana Melnik, an associate in Dickinson Wright's Ann Arbor office, can be reached at 734.623.1713 or tmelnik@dickinsonwright.com

In a June 7 press release, the Federal Trade Commission (FTC) announced two proposed consent orders – one against a debt collection firm and the other against an auto dealership – for violations involving the public disclosure of private consumer information, including Social Security numbers. In both instances, the data breaches occurred because peer-to-peer (P2P) file sharing software was installed on company computers, which made data on a person's computer available to everyone else connected to that P2P network.

One of the two actions is against EPN, Inc., a debt collector based in Provo, Utah, which provides services to healthcare providers and other clients. The FTC alleges that EPN's chief operating officer installed P2P file sharing software on the company's network, causing the disclosure of Social Security numbers, health insurance numbers and medical diagnosis codes of 3,800 hospital patients. The software was disabled in April 2008, "when EPN was informed by a client that two files containing personal information about the client's debtors were available on a P2P network." The FTC found that, using healthcare terms, EPN had failed to perform a risk assessment and address deficiencies. As such, the FTC found EPN's actions constituted unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act.

The other action is against Franklin's Budget Car Sales, Inc., also d/b/a Franklin Toyota/Scion, out of Statesboro, Georgia. In this case, records for 95,000 individuals were made available on a P2P network, which included names, addresses, Social Security Numbers, birth dates, and driver's license numbers. The FTC noted that while the dealership advised consumers through a privacy policy that it "maintain[s] physical, electronic, and procedural safe guards that comply with federal regulations to guard non public personal information," the dealership failed to have appropriate safeguards in place. The FTC found that the dealership violated Section 5(a) of the FTC Act, Title V, Subtitle A of the Gramm-Leach-Bliley Act, the FTC's Privacy of Customer Financial Information Rule, and the FTC's Standards for Safeguarding Customer Information Rule.

The punishment from the FTC tends to be for a longer period of time than what the Office of Civil Rights doles out in similar circumstances: each company must undergo a security risk assessment from a qualified security professional within the first 180 days after service of the order, and each 2 year period thereafter for 20 years. Although under some circumstances, the FTC will also fine companies, this did not appear to take place in these cases.

The consent agreements are subject to public comment for 30 days (available through July 9), after which the FTC will decide whether to make the proposed consent orders final.

Both the FTC and OCR have made clear that companies that handle sensitive information must take steps to ensure that data is secure. Best practices suggest that a risk assessment must be undertaken on an annual basis and yet again if changes are made in the network infrastructure (e.g., purchase and integration of new equipment, transition to a new data center, closing of an office, etc.).

TO BE BYOD OR NOT TO BE BYOD: IS A "BRING YOUR OWN DEVICE" POLICY RIGHT FOR YOUR ORGANIZATION?

By Tatiana Melnik, • tmelnik@dickinsonwright.com

For years, many healthcare organizations have opted to purchase mobile devices for their employees. But due to the rapid changes in the mobile market and the negative feedback from employees, many healthcare organizations have decided to permit their employees to use their own mobile devices for work purposes. However, is this policy appropriate for your organization?

IBM recently announced that due to privacy and security concerns, it had banned the use by its employees of Siri, the personal assistant that comes standard on the iPhone 4S. These concerns arise because of the way the Siri software processes requests – it sends them back to Apple. That is, when people speak a command into Siri or ask Siri a question, according to the Licensing Agreement, "the things you say will be recorded and sent to Apple in order to convert what you say into text and . . . to also process your requests." Similarly, IBM has banned Apple's Dictation tool because it can be used to take dictation for text messages and emails. For organizations that have protected health information or other sensitive information (e.g., trade secrets), this process may create problems.

Many organizations adopted Bring Your Own Device policies in an effort to minimize costs and to increase employee efficiency. However, employers must be careful to ensure that the devices used by employees do not contain apps that lead to increased security concerns.

As such, employers who have adopted Bring Your Own Device policies should take the opportunity to audit the devices for compliance with their policies. Additionally, each device should include technology that permits it to be wiped remotely if it is lost and employees should sign an acknowledgment that their device will be wiped if lost. While employees do like using their own devices, a BYOD approach will likely not be appropriate for all healthcare organizations. Organizations that continue down this path should consider refinement of their Bring Your Own Device policies to be more in the nature of "Bring Your Own Pre-Approved Device if You Use it on Our Terms."

Dickinson Wright Offices

Detroit
500 Woodward Avenue
Suite 4000
Detroit, MI 48226
Phone: 313.223.3500

Lansing
215 S. Washington Square
Suite 200
Lansing, MI 48933
Phone: 517.371.1730

Ann Arbor
350 S. Main Street
Suite 300
Ann Arbor, MI 48104
Phone: 734-623-7075

Troy
2600 W. Big Beaver Rd.
Suite 300
Troy, MI 48084
Phone: 248.433.7200

Grand Rapids
200 Ottawa Avenue, NW
Suite 1000
Grand Rapids, MI 49503
Phone: 616.458.1300

Washington, D.C.
1875 Eye Street, NW
Suite 1200
Washington, DC 20006
Phone: 202.457.0160

Toronto
222 Bay Street, 18th Floor
PO Box 124
Toronto, ON, Canada M5K 1H1
Phone: 416.777.0101

Nashville
424 Church Street
Suite 1401
Nashville, TN 37219
Phone: 615.244.6538

Phoenix
5009 East Washington Street
Suite 125
Phoenix, AZ 85034
Phone: 602.244.1400

Las Vegas
7201 West Lake Mead Blvd.
Suite 503
Las Vegas, NV 89128
Phone: 702.541.7888