

HEALTHCARELEGALNEWS



April 13, 2012 • Volume 2, Number 3

HEALTHCARELEGALNEWS EDITORIAL BOARD

Kevin M. Bernys,
248.433.7234 • kbernys@dickinsonwright.com

James L. Hughes,
734.623.1940 • jhughes@dickinsonwright.com

Neil B. Krugman,
615.620.1701 • nkrugman@dickinsonwright.com

Ralph Levy, Jr.,
615.620.1733 • rlevy@dickinsonwright.com

IN THIS ISSUE

Data Breach Issues Continue to Take Center Stage - Michigan is the Second State to See a Data Breach Class Action; OCR Issues First Penalty under HITECH

Litigation News

Recent Case Illustrates Need for Care in Drafting Physician Employment Agreements

Reimbursement News

Physicians Need to Use Caution When Reassigning Medicare Payments

Disclaimer: Healthcare Legal News is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of healthcare law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in Healthcare Legal News.

DW HEALTHCARE TEAM - NEWS & SUCCESS STORIES

Out Now

- Ralph Levy authored *Beware the Super-Bundle: Medicare Pilot Program on Bundled Payments to Health Care Providers Could Be the Next PPS for Dialysis*, published in *Nephrology News & Issues* (Feb. 2012).
- 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)

On **May 8**, Brian Balow and Tatiana Melnik will be speaking on *Impacts of FDA Regulations On Mobile Health Apps* at a Webinar hosted by Online Tech. Please contact Tatiana at tmelnik@dickinsonwright.com if you are interested in additional details on this Webinar.

On **June 28**, Brian and Tatiana will be speaking on the legal issues surrounding mobile health at the Health IT Innovation Summit – mHealth in California.

DATA BREACH ISSUES CONTINUE TO TAKE CENTER STAGE

Michigan is the Second State to See a Data Breach Class Action; OCR Issues First Penalty under HITECH



By Brian R. Balow, who is a member in Dickinson Wright's Troy office and can be reached at 248.433.7536 or bbalow@dickinsonwright.com

As we predicted in an article in our December 2011 issue, actions stemming from data breaches have increased in the first quarter of 2012. So far this year we have seen an increase in class action litigation and enforcement activity from the Office of Civil Rights.

Class Action - Sutter Health

In our December issue, we discussed the class action filed in California against Sutter Health, Sutter Medical Foundation, Sutter Physician Services, and Does 1 - 100, in connection with an October 2011 data breach from the theft of a password-protected, unencrypted computer, alleging violations of California's Confidentiality of Medical Information Act and California's breach notification law. This computer contained data on over 4 million patients. Since the initial filing in December, an additional 12 class actions were filed in California as a result of this same incident. In an effort to conserve judicial resources, the Judicial Council of California combined

the 13 class actions in February. Since then, we have seen little additional activity.

California's pro-consumer environment provides an attractive test bed for private lawsuits related to data security breaches. Although in December, we anticipated that these California actions would get further along before similar actions appeared in other states, so far, this has not been the case.

Class Action - Henry Ford Health System

In February, Michigan became the second state to have a data breach class action lawsuit filed when the Henry Ford Health System ("Henry Ford") was sued for an alleged data breach that occurred at a medical transcription provider. According to the complaint, Henry Ford mailed a breach notification letter to the "named" Plaintiff (as "Jane Doe") in January 2010. In the letter, attached as an exhibit to the complaint, Henry Ford explained that the affected patient's data was visible on the Internet. Henry Ford learned of the data breach on November 29, 2009, and had the Plaintiff's information removed from public display by December 4, 2009. Henry Ford explained that it "is unable to determine exactly how long the information was visible online, however there is no proof it was viewed or used inappropriately." Part of the information allegedly disclosed was that the Plaintiff had a sexually transmitted disease.

This lawsuit seeks damages for (i) invasion of privacy through a public disclosure of per se embarrassing private facts and (ii) negligence. In Michigan, a plaintiff must prove actual damages to recover under a negligence claim, but in a claim of public disclosure of private facts, emotional distress and mental anguish may be enough.

HHS/OCR HITECH Action - Blue Cross Blue Shield of Tennessee

Most recently, on March 13, 2012, the Department of Health and Human Services (HHS), Office of Civil Rights (OCR) issued its first enforcement action stemming from the HITECH Act Breach Notification Rule based on an incident in which protected health information of more than 1 million patients was disclosed. Blue Cross Blue Shield of Tennessee (BCBST) agreed to pay HHS \$1.5 million to settle potential violations of the HIPAA Privacy and Security Rules. BCBST further agreed to a corrective action plan to address gaps in its HIPAA compliance program.

The OCR enforcement action stemmed from a Breach Notification Report submitted by BCBST on November 3, 2009. On October 5, 2009, BCBST employees discovered a theft of computer equipment from a network data closet located in Chattanooga, TN. The facility was managed by a third party management firm, but according to BCBST the closet was secured by both biometric and keycard scan security with a magnetic lock and an additional door with a keyed lock. BCBST's internal investigation found that the theft occurred on or about October 2, 2009. The stolen items included 57 hard drives containing encoded electronic data, consisting of over 300,000 video recordings and over 1 million audio recordings of customer service calls. The drives contained names of BCBST plan members, social

security numbers, diagnosis codes, dates of birth, and health plan identification numbers.

OCR initiated its investigation on January 8, 2010. According to OCR, its investigation indicated BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.

The Resolution Agreement explicitly states that BCBST did not admit and expressly denies any liability as a result of the theft.

LITIGATION NEWS

RECENT CASE ILLUSTRATES NEED FOR CARE IN DRAFTING PHYSICIAN EMPLOYMENT AGREEMENTS



By Ralph Levy, Jr., who is Of Counsel in Dickinson Wright's Nashville office, and can be reached at 615.620.1733 or rlevy@dickinsonwright.com

In a recent non-precedential decision, the Third Circuit Court of Appeals affirmed a lower court decision that a physician's employment agreement could be terminated by his former employer without cause. In reaching its decision, the Court rejected the physician's reliance on an offer letter that he received prior to his execution of an employment agreement. In this letter, his prospective employer indicated that the physician would be given a specified time period to obtain board certification in the United States for the specialty for which he was to be employed.

Geisinger Clinic recruited Philip Edwards, a UK-trained and licensed physician who specialized in interventional radiology, to join its employ. Although Geisinger's policy was to require any newly employed physician to be U.S. board certified for the specialty that the physician was being employed, in Edwards' case, the Geisinger Clinic indicated that it would allow Edwards to begin employment, but that he was to obtain his board certification within a four to six year period. Despite an offer letter and other correspondence between the physician and his employer that referred to this time period within which Edwards was to obtain U.S. board certification, his employment agreement did not contain any references to this time period or requirement. Moreover, the agreement provided that Edwards' employment could be terminated at any time by the Geisinger Clinic with or without cause. Approximately one year after Edwards began work, Geisinger Clinic terminated his employment.

Edwards sued his former employer for breach of the employment contract. The trial court granted Geisinger Clinic's motion for summary judgment and found that as a matter of law, the employment

agreement allowed Edwards' employment to be terminated at any time without cause. In upholding the trial court's decision, the appellate court concluded that any references in the pre-employment offer letter as to the time period for Edwards to obtain US board certification did not guarantee Edwards' employment by the Geisinger Clinic for any minimum time period.

Physicians and their employers can learn several lessons from the Edwards case. First, care should be taken in drafting termination clauses in a physician employment agreement. The agreement should clearly state whether either or both of the employer and/or the employee can terminate employment, and if so, the terms and/or conditions of any such termination. In addition, the contract should indicate whether any advance notice is required prior to termination, and if terminable for "cause", the agreement should include a detailed definition of what constitutes "just cause." Finally, the agreement should also address the impact of termination of the employment agreement on any remaining obligations imposed under the agreement such as noncompetition, nonsolicitation and nondisclosure. For example, if the employer terminates the agreement without cause, will the physician continue to be bound by the noncompetition covenant that applied while the employment agreement was in effect?

The second lesson to be learned is that a physician employment agreement should indicate in clear and unambiguous language that all prior offers and discussions are "merged into" the employment agreement. Perhaps if the employment agreement in Edwards stated that the employment agreement superseded the offer letter by the Geisinger Clinic to Edwards, litigation could have been avoided. (The Court of Appeals in Edwards did not indicate whether the employment agreement contained such a "supersedence" clause). In drafting physician employment agreements, the best practice is for the supersedence clause to make a specific reference to the date(s) of the prior offer letters and/or summary of terms that are being superseded and "merged into" the employment agreement.

REIMBURSEMENT NEWS

PHYSICIANS NEED TO USE CAUTION WHEN REASSIGNING MEDICARE PAYMENTS



By Kevin Bernys, who is a member in Dickinson Wright's Troy office, and can be reached at 248.433.7234 or kbernys@dickinsonwright.com

The Office of Inspector General (OIG), which is the enforcement arm of HHS, recently issued an Alert to physicians to exercise caution when reassigning their rights to Medicare payments. Physicians who reassign their right to bill and receive payments from Medicare may be liable for false claims submitted by the person to whom they reassigned their rights.

By way of background, Medicare pays suppliers (i.e., physicians or non-physician practitioners) for covered services if the beneficiary (i.e., the

patient) assigns the claim to the suppliers, and the suppliers accept assignment. By accepting assignment, physicians agree (among other things), to accept as full payment for the services the amount approved by the carrier as the Medicare Part B payment (i.e., the reasonable charge or the lesser of the fee schedule amount and the actual charge), and to limit charges to the patient and other sources as required under the federal regulations.

Title XVIII of the Social Security Act prohibits payment for services provided by physicians to be paid to another individual or supplier, unless the physicians authorize such payment to be made to a permissible person. Medicare will pay the physicians' employer if physicians are required, as a condition of employment, to turn over to the employer the fees for the physicians' services. Medicare will also pay an entity enrolled in the Medicare program if there is a contractual arrangement between the entity and the physicians under which the entity bills for the physicians' services. In either case, this is considered a "reassignment" of the right to bill Medicare and receive payment from Medicare, and in each case, the employer or entity entitled to receive payment is considered the "supplier" of the services rendered. Medicare will also pay an agent who furnishes billing and collection services to physicians or to their employer if certain requirements are satisfied, but the payment to the agent is made in the name of the physician or the employer or entity who engages the agent.

Under the reassignment rules, an entity enrolled in the Medicare program that receives payment under a contractual arrangement, and the supplier that otherwise receives payment, are jointly and severally responsible for any Medicare overpayment to that entity. Moreover, nothing in the exceptions to the prohibition on the payment to another person for services rendered by a physician alters a party's obligations under the anti-kickback section of the Social Security Act, the physician self-referral prohibition section of the Act, the rules regarding physician billing for purchased diagnostic tests, the rules regarding payment for services and supplies incident to a physician's professional services, or any other applicable Medicare laws, rules or regulations.

A recent OIG Alert encourages physicians to scrutinize employers and entities to whom they reassign their right to bill Medicare to be certain they are legitimate providers or suppliers of healthcare items and services and that they are properly billing Medicare for the physicians' services or when using the physicians' provider number.

Specifically, the OIG Alert reports that the OIG recently reached settlements with 8 physicians who violated the Civil Monetary Penalties Law by causing the submission of false claims to Medicare from physical medicine companies. In each case, the physician assigned his/her Medicare payments to a physical medicine company in exchange for a medical directorship position with such company. In such a role, these physicians did not personally render or directly supervise any services, but the companies billed Medicare using the physician's reassigned provider number claiming services were rendered by the physician when in fact they were rendered by someone else (unlicensed

technicians). The OIG pursued action against the physicians and the company owners.

Under federal law, the physician (or supplier) who furnishes the service has “unrestricted access to claims submitted by an entity for services provided by that supplier.” This right to access applies irrespective of whether the physician or other supplier is an employee or whether the service is provided under a contractual arrangement. If a request to provide the billing information to the physician or supplier performing the service is denied, CMS may revoke the entity’s right to receive reassigned benefits.

Thus, it is important that all physicians and suppliers periodically review the billings submitted by others on their behalf, whether following a reassignment or simply hiring an outside billing company to handle the billing, because both the one to whom the billing number is issued and the one who allegedly provided the services may be liable for false or inaccurate billing for such services.

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

301 East Liberty Street
Suite 500
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