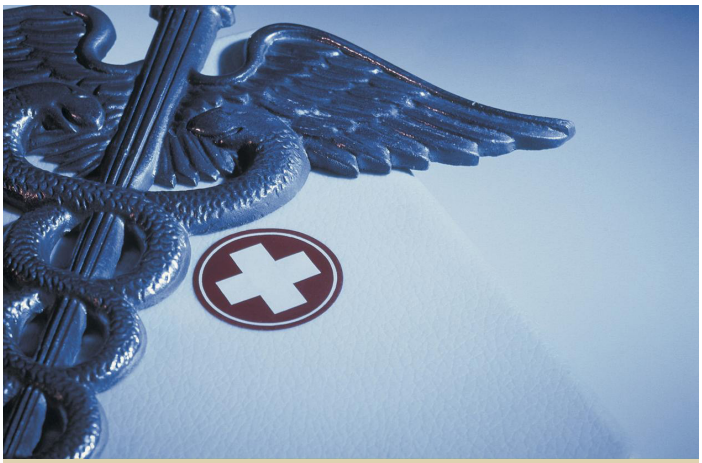

September 2014 • Volume 4, Number 3

IN THIS ISSUE

DW HEALTHCARE BLOG
http://www.dwhealthlawblog.com/

DICKINSON WRIGHT'S

HEALTHCARE **LEGAL**NEWS

Special Issue: HIPAA Update

REGISTER NOW! SPACES STILL AVAILABLE FOR OUR UPCOMING EVENTS

ARE YOU HIPAA-NOTIZED YET?
The Latest Insights and Developments

Friday, September 19, 2014
Prince Conference Center at Calvin College
1800 East Beltline SE
Grand Rapids, MI | 49546-5951
Registration & Continental Breakfast | 7:30AM
Seminar | 8:00 - 11:00AM

Friday, September 26, 2014
Bank of America Building
2600 West Big Beaver Road
Troy, MI | 48084-3312
Registration & Continental Breakfast | 7:30AM
Seminar | 8:00 - 11:00AM

Topics will include:
- Basic privacy and security requirements
- Practical tips for HIPAA compliance
- New rules for notice of privacy practices, business associates and breach notification
- Responding to subpoenas and other requests for health information
- HIPAA enforcement: past, present and future

Please RSVP to Mellissa Boyd at 313.223.3125 or mboyd@dickinsonwright.com.

RECENT TRENDS IN HIPAA LIABILITY
by Scott F. Roberts, who is Of Counsel in Dickinson Wright's Troy office

Since the passage of the 2013 HIPAA Omnibus Rule, there has been a substantial increase in HIPAA enforcement actions brought by the Department of Health and Human Services, including an increase in so-called "high-impact cases" where settlements can reach into the millions of dollars. In addition, while HIPAA does not provide for a private cause of action, plaintiffs' lawyers are increasingly characterizing unauthorized disclosures of electronic protected health information ("ePHI") as violations of the Fair Credit Reporting Act ("FCRA"), which provides plaintiffs with a private cause of action. Accordingly, it is more important than ever that providers ensure that their data protection measures comply with the standards set forth in the HIPAA Security Rule.

One common issue in HIPAA compliance is the existence of portable media, particularly laptops containing ePHI. Theft of portable electronic devices accounts for around half of the health data breaches that HHS typically faces. By comparison, hacking and IT incidents only account for around ten percent of HHS cases. Just this year, two healthcare entities paid a combined $1,975,220 to HHS after two laptops containing ePHI were stolen. In the first instance, an unencrypted laptop containing the ePHI of 148 individuals was stolen from an employee's car. In the other instance, as a result of a theft of an unencrypted laptop from the provider's facility, the provider paid $1,725,220 in fines. Multiple risk analyses performed by the provider recognized this problem, but the provider did not take sufficient steps to prevent it from happening.

The second most common issue is unauthorized access or disclosure of protected health information. This type of disclosure is of particular concern due to recent attempts by plaintiffs' attorneys to seek damages for unauthorized disclosure under the FCRA. Such a case was recently brought against the University of Miami. In that case, the University transferred its patients' ePHI to a third party vendor to store offsite. Employees of the vendor or other individuals with access to the vendor's servers accessed the University's ePHI and then sold the information to various scam artists. The ePHI that was stolen included names, birthdates, and social security numbers. While the case is still pending in U.S. District Court for the Southern District of Florida, if plaintiffs are successful, the potential damages could easily reach into the millions or even tens of millions of dollars.

In sum, plaintiffs' lawyers are now looking at violations of HIPAA as potential causes of action under the FCRA, and HHS is taking patient privacy more seriously than ever. The important take away for healthcare providers is that they too must consider patient privacy to be a grave concern or face ever increasing liability under HIPAA and possibly even the FCRA.

HIPAA VIOLATION RESULTS IN $4.8 MILLION SETTLEMENT: AN IT PERSPECTIVE

by Jared A. Smith, who is an Associate in Dickinson Wright's Troy office, and can be reached at 248.433.7597 or jsmith@dickinsonwright.com

In today's healthcare industry, information technology ("IT") systems play an ever-expanding role in the success of a medical practice. Medical practitioners consistently juggle e-billing and electronic medical records software risk, HIPAA compliance issues, data security and data privacy requirements and meaningful use thresholds, all of which are typically addressed in IT vendor agreements. Further, IT vendors are often willing to accept significant revisions to their standard contracts, and well-negotiated and properly structured relationships with IT vendors can protect medical practices from disaster in the event of an IT system failure like the one outlined below.

In our previous issue of Healthcare Legal News, Rose Willis described a record-setting fine imposed on New York-Presbyterian Hospital ("Hospital") and Columbia University Medical Center ("Columbia") for HIPAA violations associated with their IT infrastructure. Specifically, a Columbia doctor inadvertently disclosed the electronic protected health information ("ePHI") of about 7,000 patients to Google and other easily-accessible search engines when he deactivated his personally owned server from the Columbia network. The Hospital and Columbia learned of the data security breach when they received a complaint from an individual who discovered the ePHI of the individual's deceased partner through a simple internet search, and the Hospital and Columbia then self-reported the breach to the Department of Health and Human Services Office for Civil Rights ("OCR"). At the conclusion of OCR's investigation into the breach, the Hospital and Columbia agreed to enter into a settlement and a Corrective Action Plan that required the payment of $4.8 million to OCR, the largest settlement for HIPAA security violations to date.

Aside from the extent of the breach—almost 7,000 patients' ePHI exposed to anyone with internet access—the size of the settlement can be attributed to two major failures on the part of the Hospital and Columbia. First, the Hospital and Columbia lacked sufficient IT safeguards, which permitted a single doctor to accidentally expose the ePHI of such a large number of patients. Generally, a medical practice's IT infrastructure should not be structured in a way that permits one person to accidentally compromise the entire system's security, and a strong IT services agreement with a reputable IT vendor is an important first step in avoiding such a scenario. The best IT vendors work closely with their clients to implement IT safeguards tailored to each distinct medical practice, and a negotiated IT vendor contract should appropriately allocate data security risk between the medical practices and the IT vendors.

Second, the Hospital and Columbia failed to perform a sufficiently thorough risk analysis of their IT systems. Under the HIPAA Security Rule, most healthcare providers are required to conduct a risk analysis of their IT equipment to determine where data security vulnerabilities exist and how to effectively address them. Here, the Hospital and Columbia did, in fact, conduct risk analyses, but OCR determined that their risk analyses did not adequately address their particular data security issues. Again, experienced IT vendors collaborate with their clients so that data security vulnerabilities are discovered, and the risk analysis obligations of the applicable medical practice and the IT vendor should be well-defined in a negotiated IT vendor agreement.

HIPAA OMNIBUS RULE: DEADLINE APPROACHING TO UPDATE GRANDFATHERED BUSINESS ASSOCIATE AGREEMENTS

by Billee Lightvoet Ward, who is Of Counsel in Dickinson Wright's Grand Rapids office, and can be reached at 616.336.1008 or bward@dickinsonwright.com

Although the HIPAA Omnibus Rule (the "Rule") went into effect nearly 18 months ago, the transition period for bringing business associate agreements into compliance with the Rule's new requirements will end on September 23, 2014. Business associates were directly regulated and responsible for complying with the Rule as of September 23, 2013, but the Rule provided for a one-year transition period for certain business associate agreements that were in place prior to January 25, 2013 (the date the Rule was published). As of September 23,

2014, all business associate agreements must reflect the Rule's new requirements. Those requirements include the following:

- Require that the business associate comply, and require its subcontractors to comply, with applicable requirements of the Security Rule;
- Require that the business associate ensure that its subcontractors agree to the same restrictions and conditions that apply to the business associate with respect to protected health information;
- Require that the business associate report breaches of unsecured protected health information to the covered entity;
- If the business associate carries out a covered entity's obligation under the Privacy Rule, require that the business associate comply with the Privacy Rule requirements that apply to the performance of such obligation; and
- Require the business associate take steps to cure or end the violation (or terminate the relationship) if it knows of a pattern of activity or practice of its subcontractor that constitutes a material breach of the subcontractor's obligations.

This upcoming deadline serves as a good reminder for covered entities and business associates to review, amend or replace existing business associate agreements. In addition, this deadline reminds covered entities of their obligation to exercise diligence in establishing and monitoring their business associate relationships going forward.

The Rule made sweeping changes to the concept of business associates by expanding the definition to include subcontractors who create, receive, maintain or transmit protected health information on behalf of a business associate; health information organizations, e-prescribing gateways, and certain other persons that provide data transmission services for covered entities; and persons that offer personal health records on behalf of a covered entity. Because the definition of business associate has been expanded to include many vendors who were not previously regulated by HIPAA, covered entities and business associates may need to educate downstream service providers on HIPAA's applicability and required contract language. The parties may wish to negotiate additional terms such as insurance and indemnification provisions to allocate risks in light of their respective compliance obligations.

EX PARTE COMMUNICATIONS BETWEEN TREATING PHYSICIAN AND ATTORNEYS

by Keith C. Dennen, who is a Member in Dickinson Wright's Nashville office, and can be reached at 615.780.1106 or kdennen@dickinsonwright.com

Under HIPAA, physicians are permitted to disclose "protected health information" to their attorneys for purposes of their own healthcare operations. This allows physicians sued by patients for malpractice to provide their attorneys with the information needed to prepare and present a defense. Ordinarily, subpoenas or orders are a part of a court ordered deposition or trial at which the patients or their attorneys are present, so the need to protect health information is lessened.

HIPAA does not allow treating physicians in one practice to disclose "protected health information" to attorneys for a treating physician in another practice unless a subpoena or an order of a court permits that disclosure. Instead, HIPAA allows members of a group practice to transmit protected health information concerning a patient to business associates of that practice. This means that attorneys representing the other physicians in the group practice can receive information related to the practice's healthcare operations, including information relating to representing the practice in malpractice lawsuits. A subpoena or court order is not required for this disclosure. Thus, when a physician is being sued for malpractice, HIPAA permits the practice's attorney to meet with other physicians in that same practice and obtain protected health information related to the plaintiff.

While HIPAA may permit the disclosure of protected health information in this circumstance, state law is another matter altogether. For example, the Tennessee Supreme Court found that an implied covenant of confidentiality exists between the treating physician and his or her patient. Like HIPAA, this implied covenant of confidentiality absolutely prohibits an attorney for a treating physician from meeting with another treating physician unless the patient or the patient's attorney is present. Like HIPAA, the court assumes that the patient's interests are protected when the patient is present.

This in turn begs the question—does the implied covenant of confidentiality prohibit a physician employed in a group practice from meeting with the attorneys representing another employee of the practice who has been sued for malpractice without the patient being present? In Tennessee, this issue was recently addressed in *Hall v. Crenshaw*, W2013-00662-COA-R9-CV (Tenn. Ct. App. July 18, 2014). The court of appeals in *Hall* held that the implied covenant of confidentiality does not prohibit a physician in a group practice from meeting with attorneys representing another employee physician of the practice. The court of appeals reasoned that a corporation can only function through its agents and employees. Under state law, all knowledge of the corporation's employees is imputed to the corporation. As a result, the court held that the corporation already possessed this information, meaning the corporation, through its employees, is able to discuss a patient's medical record and history with the attorneys representing the corporation and its employees.

COMPLYING WITH RECENT CHANGES TO THE PHYSICIAN'S NOTICE OF PRIVACY PRACTICES

by Rose J. Willis, who is a Member in Dickinson Wright's Troy office, and can be reached at 248.433.7584 or rwillis@dickinsonwright.com

A physician practice's Notice of Privacy Practices ("NPP") acts as the "roadmap" to the practice's permitted uses and disclosures of their patients' protected health information ("PHI"). September 23, 2013 was the deadline for revising NPPs to comply with the changes set forth in the 2013 HIPAA Omnibus Final Rule, meaning that any NPPs

not so revised as of the date of this article are already past due. This article explains some of the changes made to the content of NPPs under the Final Rule, to assist the physician practice with confirming that necessary changes have been made.

- Each NPP must expressly state that the following actions require an individual's written authorization: (i) any uses and disclosures of PHI for marketing purposes and (ii) any sale of PHI by the practice.
- If the practice records or maintains psychotherapy notes, then its NPP must include a statement that uses and disclosures of psychotherapy notes require an individual's written authorization.
- If the physician practice intends to contact an individual for fundraising purposes, the physician practice must disclose in its NPP that it may contact the individual to raise funds, and specify that the individual has the right to opt out of receiving such communications.
- The NPP must include a statement that the affected individuals will be notified in the event of a breach of their unsecured PHI.

- The NPP must inform individuals of their right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service.

Additionally, because these revisions are considered "material", upon making these changes each practice must advise their existing patients of the change by providing a copy of the revised version at the patient's next appointment. If the practice maintains the NPP on its website, the revised version must be promptly posted.

For more information on these changes, attend Dickinson Wright's HIPAA seminar "Are you HIPAA-notized Yet?"

DICKINSON WRIGHT OFFICES

Detroit
500 Woodward Ave.
Suite 4000
Detroit, MI 48226
Phone: 313.223.3500

Ann Arbor
350 S. Main St.
Suite 300
Ann Arbor, MI 48104
Phone: 734.623.7075

Columbus
150 E. Gay St.
Suite 2400
Columbus, OH 43215
Phone: 614.744.2570

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

Las Vegas
8965 South Eastern Ave.
Suite 280
Las Vegas NV 89123
Phone: 702.382.4002

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

Nashville
424 Church St.
Suite 1401
Nashville, TN 37219
Phone: 615.244.6538

Saginaw
4800 Fashion Square Blvd.
Suite 300
Saginaw, MI 48604
Phone: 989.791.4646

Phoenix
1850 North Central Ave.
Suite 1400
Phoenix AZ 85004
Phone: 602.285.5000

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

Toronto
199 Bay St., Suite 2200
Commerce Court West
Toronto ON M5L 1G4
Phone: 416.777.0101

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