Wisconsin Society for Healthcare Risk Management

Risky Business

Issue 77 • December 2013

Not Hip to HIPAA? Could Lead to Pain in the Pocketbook

By Stephane P. Fabus
and Katherine A. Kuchan

As of September 23, 2013, sweeping changes to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") took effect, impacting how both covered entities, such as health care providers, health plans and health care clearinghouses, and their business associates, which includes many of the covered entities' contractors and subcontractors, handle protected health information ("PHI"). The HITECH Final Rule, originally issued on January 25, 2013, implements the statutory changes required by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, plus other changes initiated by the Office for Civil Rights ("OCR"). A copy of the HITECH Final Rule may be accessed at the website. As demonstrated by the settlements described below, non-compliance with these new HIPAA requirements could mean big penalties for covered entities and their business associates. A summary of key changes impacting HIPAA is provided at the end of this article.

Recent Settlements

In the first nine months of 2013, OCR, which is charged with enforcing HIPAA compliance, has already entered into four resolution agreements to settle alleged violations of both the HIPAA Privacy and Security Rules, located at Parts 160 and 164 of Title 45 of the Code of Federal Regulations.

In May, a university in Idaho (the "University") agreed to pay the U.S. Department of Health and Human Services ("HHS") $400,000 to settle allegations that it violated the HIPAA Security Rule. The allegations involved the breach of the confidentiality of the unsecured electronic PHI of approximately 17,500 patients at one of the University's clinics. The PHI had been unsecured for at least ten months due to disabled firewall protections on servers maintained by the University. OCR alleged that the University's risk analyses and assessments of its clinics were incomplete and did not adequately identify potential vulnerabilities and risks. OCR also alleged that the University failed to assess the likelihood of potential risks and that it could have detected the firewall breach sooner had it applied proper security measures, policies and procedures, as are required by HIPAA. This settlement emphasizes the importance of routine reviews of information systems and ongoing risk analysis and management as part of an effective HIPAA security compliance program.

In June, a large regional medical center located in California (the "Medical Center"), entered into a settlement with HHS for $275,000 to resolve allegations that it violated the HIPAA Privacy Rule. OCR began a compliance review of the Medical Center following publication of a Los Angeles Times article indicating that two Medical

continued on p. 2

HIPAA, *cont. from p. 1*

Center senior leaders discussed medical services provided to a patient with the media. OCR indicated that the Medical Center failed to safeguard the patient's PHI from impermissible disclosure, in violation of the HIPAA Privacy Rule, by intentionally disclosing the PHI to various media outlets on multiple occasions without a valid patient authorization. Under the HIPAA Privacy Rule, PHI can only be disclosed in limited circumstances absent an authorization; in all other instances, an authorization must be obtained prior to the disclosure.

In addition, according to OCR, the Medical Center's senior leadership impermissibly circulated an email to the entire workforce that included details regarding the patient's medical condition and failed to sanction workforce members in accordance with its sanctions policy for the impermissible disclosure. In addition to the monetary settlement, OCR required fifteen other entities under the same ownership or operational control as the Medical Center to attest to understanding the types of uses and disclosures of PHI that are permissible under HIPAA.

This settlement emphasizes the important role that senior leadership plays in fostering a culture of HIPAA compliance within an organization. Senior leadership is responsible for knowing, understanding, and complying with HIPAA Privacy and Security Rules to ensure protection of patient's rights and will be held accountable by OCR for violations.

Under the HIPAA Privacy Rule, protected health information can only be disclosed in limited circumstances absent an authorization; in all other instances, an authorization must be obtained prior to the disclosure.

In July, HHS announced a $1.7 million settlement with a health benefits company based in Indianapolis, Indiana (the "Company"), to resolve allegations that the Company violated both the HIPAA Privacy and Security Rules. HIPAA requires entities to self-report known breaches of unsecured PHI directly to HHS. This settlement arose from such a breach report submitted by the Company when it discovered that security weaknesses in its online database left 612,402 individuals' electronic PHI vulnerable to access by unauthorized persons over the Internet for over four months. According to OCR's investigation, the Company did not implement appropriate administrative and technical safeguards, which are, in addition to physical safeguards, required under HIPAA. This case sends a strong warning to covered entities to take caution whenever implementing changes to information systems, particularly when Web-based applications or portals are involved that provide access to PHI through the Internet. Further, as of September 23, 2013, business associates who perform services, including these types of systems upgrades, for, or on behalf of, covered entities can be directly liable to HHS for not having adequate physical, technical and administrative safeguards in place.

In August, a not-for-profit managed care plan in New York (the "Plan"), agreed to a settlement with HHS exceeding $1.2 million for alleged violations of the HIPAA Privacy and Security Rules. The Plan filed a breach report after being informed by a CBS Evening News representative that, as part of an investigatory report, CBS had purchased a photocopier previously leased to the Plan and discovered that its hard drive still contained confidential medical information. An estimated 344,579 individuals' PHI was implicated by the breach. OCR's investigation found that the Plan had not incorporated the storage of electronic PHI on copier hard drives into its risk and vulnerabilities analysis, and failed to implement policies and procedures regarding the return of copiers to leasing agents, in violation of the Security Rule. This case emphasizes the importance of assessing the HIPAA implications related to equipment designed to retain electronic information and implementing policies and procedures to ensure hardware is wiped clean of personal information prior to return, destruction or recycling.

In addition to paying the settlements listed above, these four covered entities were also required to enter into corrective action plans with OCR to address the deficiencies leading to

continued on p. 3

their respective alleged HIPAA violations.

The number of HIPAA violations resulting in settlement has steadily increased each year since the first HIPAA settlement in 2008. To date, there have been fifteen settlements and one imposition of civil monetary penalties ("CMPs") where informal resolution could not be achieved. Further, as the cases above demonstrate, there are many different types of entities that are subject to and liable for violation of the HIPAA requirements. While so far only covered entities have been the target of OCR investigations, the HITECH Final Rule expanded direct liability to business associates. Therefore, it is important that business associates ensure HIPAA compliance or risk being the target of OCR enforcement action.

Recent Key Changes to HIPAA

Many new changes to HIPAA addressed in the HITECH Final Rule became effective as of September 23, 2013. A summary of key changes and their related provisions is outlined below. Please note, however, that other state and federal laws governing the confidentiality of information must also be considered in implementing appropriate security and privacy measures. Any federal or state law offering greater protection preempts a HIPAA requirement requiring less protection.

Business Associates. In addition to covered entities, business associates are now directly liable for compliance with the HIPAA Security Rule and most of the Privacy Rule. The definition of "business associate" was expanded to explicitly include several types of entities and specify that creating, receiving, maintaining or transmitting PHI on behalf of a covered entity will trigger business associate-status. Examples of some entities that may fall into the business associate category include patient safety organizations, data transmission organizations, vendors of personal health records and data storage vendors, among others. Covered entities and business associates are required to have a HIPAA-compliant business associate agreement in place, as are business associates and their subcontractors who handle PHI.

Breach Notification. Under HIPAA, "breach" means the acquisition, access, use or disclosure of unsecured PHI not permitted by the Privacy Rule unless there is a low probability the PHI has been compromised based on a risk assessment. A breach is to be presumed until a risk assessment proves otherwise. Business associates are required to notify covered entities of discovered breaches, security incidents or unauthorized uses and disclosures of PHI in their possession. In certain instances, HIPAA requires covered entities to notify HHS, individuals or the media of breaches of unsecured PHI.

Changes to Permitted Uses and Disclosures. The types of PHI that covered entities may use for fundraising activities has expanded from demographic information only, to include health insurance status, dates of service, date of birth, department of service, treating physician, and outcome information. Individuals must be notified of their ability to opt out of receiving fundraising communications without an undue burden and be permitted to opt back in to receive such communications. Regarding marketing, generally, PHI may only be used to make communications about products or services that encourage the recipient to purchase or use the products or services if there is an individual authorization, or an exception applies and only permitted remuneration is exchanged. HIPAA also includes a prohibition on the exchange of PHI for remuneration unless permitted by an individual authorization or covered by an exception, such as for public health activities, treatment purposes or business associate services. Finally, regarding uses and disclosures for research purposes, research authorizations for present or future studies may now be combined with other types of authorizations so long as they clearly distinguish between conditioned and non-conditioned research components and permit the individual to opt in to the unconditioned components.

Individual Rights. Under HIPAA, individuals have expanded rights to access and amend PHI maintained in a designated record set, and obtain an accounting or restrict disclosures of their PHI. An individual's right of access includes the right to obtain an electronic copy of

continued on p. 4

Covered entities must provide a notice of privacy practices to patients and update such notice to reflect the recent changes to HIPAA. The covered entity must post the notice on its website and in its lobby, and provide a copy to new patients. The updated notice must also be made available to returning patients upon request.

PHI maintained in a designated record set in the electronic form and format specified by the individual. Individuals also have the right to have an electronic copy sent directly to another person or entity designated by the individual. Individuals also have the right to request that covered entities amend PHI maintained in a designated record set that is inaccurate or incomplete.

Regarding disclosures of PHI, covered entities are required to grant an individual's request that a claim not be submitted to the individual's health plan for services the individual paid for out-of-pocket and in-full, though other types of restriction requests may still be denied by the covered entity. Individuals also have the right to request an accounting of the disclosures of the individual's PHI made by the covered entity and its business associates. All disclosures that do not fall into an exception and occurred within the prior six years must be included in the accounting.

Finally, covered entities must provide a notice of privacy practices to patients and update such notice to reflect the recent changes to HIPAA. The covered entity must post the notice on its website and in its lobby, and provide a copy to new patients. The updated notice must also be made available to returning patients upon request.

Conclusion

HIPAA contains many requirements regarding the security and privacy of PHI that covered entities and business associates must abide by. Failure to comply can result in significant consequences, including OCR investigations, resolution and settlement agreements and the imposition of financial penalties, including CMPs. The discussion above provided a general overview of recent HIPAA changes and is not inclusive of all the requirements imposed by HIPAA. Entities should assess whether they satisfy the HIPAA definition of covered entity or business associate, and, if so, take appropriate steps to ensure HIPAA compliance within their organizations.

Stephane P. Fabus and Katherine A. Kuchan are attorneys with the firm of Hall, Render, Killian, Heath & Lyman, P.C.

From the President

As 2013 comes to an end, the time has come to pen my final President's Corner column for the Risky Business newsletter. I would like to start with retrospective recap of WSHRM's 2013 accomplishments. There is much to showcase! So, without further adieu, here we go:

2013 by the Numbers

- WSHRM applied for and received our **first** ever ASHRM grant to help offset the cost of hosting a local CPHRM exam prep course;
- **Twenty-two** risk managers attended the April CPHRM prep course that WSHRM hosted;
- **Eleven** Wisconsin risk managers obtained their CPHRM designation in 2013;
- There are now **34** WSHRM members who have achieved CPHRM designation, representing over **30%** of our **112** members;
- WSHRM applied for and received a one-time **$1,000** grant from ASHRM. We will apply these funds to assist WSHRM in broadening its membership base in 2014;
- WSHRM held **two** educational conferences with a combined attendance of **139**;
- WSHRM continues to offer cost-effective continuing education credits to our members. In 2013, we provided **16 CEUs** at a member rate of **$13.75 per CEU** and **19 CLEs** at a member rate of **$11.58 per CLE**;
- Cathie Aschenbrenner became the **first** WSHRM member to receive the WSHRM Member Achievement Award. Congratulations to Cathie on these well-deserved accolades!
- **Three** editions of the newly enhanced *Risky Business* newsletter were published in 2013;
- 2013 was also a year of transition. During the year, the WSHRM board welcomed **one** new board member (Sheridan Ryan) and elected **two** first-time Board members (Karen Whyms and Michelle Lahey-Reed) to serve on the Board in 2014. The WSHRM board has achieved a successful leadership transition of the sponsorship committee from Judi Nelson to Nancy Duran and Cindy Lusignan.

Keeping with the transition theme, a couple shout outs are in order as I wrap up this column.

The first is to incoming president **Kyle Fromm**, who led the effort to put together two amazing educational events in 2013. I know the organization will be in good hands in 2014 with Kyle at the helm.

The second shout out goes to Patti Erikson, who agreed to serve as president-elect and will chair the planning committee in 2014. There is a tremendous amount of effort behind the scenes to plan the WSHRM conferences and I am extremely pleased to have Patti back on the Board to lead this effort. I look forward to serving on the planning committee with her, as well as requesting volunteer support from the WSHRM membership so that we can continue to offer at least two educational programs a year. Welcome back, Patti!

Shout out three goes out to departing past-president board member Suzanne Soderlund. Suzanne has been a WSHRM member since 1993 and served as an active member of the planning committee as long as I can remember. She served as chapter president in 2012 and was a tremendous role model for me as I transitioned into this role. When I asked her to name the greatest benefit of being an active WSHRM member, she replied "Educational items as a new risk manager and networking as a 'seasoned' risk manager." Her advice to new healthcare risk managers: "Join WSHRM!" Sage advice indeed!

The next person I would like to recognize is Deb Schmidt, who departs the Board after six years of devoted service. Deb's been a member since 2001 and served as the membership coordinator during her six years on the Board.

continued on p. 6

President, *cont. from p. 5*

She also wrote a touching tribute to Cathie Aschenbrenner when nominating Cathie for the Member Achievement Award. She considers the friendships she has made as the greatest benefit of being an active WSHRM member. Her advice to new WSHRM members is to get involved.

And finally, a huge THANK YOU to departing Board member Judi Nelson. One of my first WSHRM memories was Judi warmly welcoming me to my first conference many, many years ago. Judi has been a WSHRM member since 1991 and has served as treasurer, president and, for the past six years, secretary. She also served as the Fall Conference sponsorship coordinator for as long as I can recall. Her response to my question about the greatest benefit she procured from her WSHRM experience is the relationships she built with her peers across the state, and the friendships that evolved from the professional relationships. She added that the networking opportunities with peers have been invaluable in the day-to-day performance of her job duties and she is firmly convinced there are no better resources than others doing this job to learn from and share with.

Judi's advice to WSHRM newbies is to get involved. Take full advantage of the resources that exist in your peers across the State of Wisconsin who do the job and have experiences and resources you can learn from. Great words of wisdom, Judi! One fond memory Judi shared with many of us, was the time she chased a bear from her facility's parking lot (do we not love the unpredictability of our risk management roles!).

Speaking on behalf of the WSHRM board, thank you Judi, Deb and Suzanne. Your many contributions were instrumental in making WSHRM an invaluable resource to the state's healthcare risk managers. We will miss you at future Board meetings, but know you will enjoy some well-earned rest and relaxation.

News 'n Notes

Renew Your Membership

It is never too early to start thinking about your 2014 WSHRM membership. Annual membership is $55 for January through December for all new and renewing members regardless of when they join. WSHRM continues to offer a 50% reduction in dues for retirees wishing to continue membership.

Introduce a Colleague to WSHRM

If you know of a healthcare risk manager who would benefit from joining WSHRM, please forward them a copy of this newsletter and introduce them to our great organization. The 2014 membership application may be found on the WSHRM website.

2014 Conferences

Spring Conference
May 2, 2014
Marriott West, Madison

Fall Conference
September 17-18, 2014
Wilderness Resort,
Wisconsin Dells

Board meetings are held the evening before the spring and fall conferences. Tentative board meeting times are 4–6:30 and any WSHRM member wishing to attend a board meeting is welcome.

Find us on Facebook

Remember to "like" WSHRM on Facebook, if you have not yet done so. It provides a wealth of information and keeps you informed of current events related to risk management, conferences and many more things.

The WSHRM website contains archived copies of the Risky Business newsletter, contact information for WSHRM board members, links to risk management resources, brochures for upcoming events and the ability to post questions.

WSHRM Board of Directors for 2014

President
Kyle Fromm
Blue Cross Blue Shield of MN
651-662-2608
kyle_a_fromm@bluecrossmn.com

President-Elect
Patti Erickson
Wheaton Franciscan Healthcare
patti.erickson@wfhc.com

Past President
Matt Wahoske
608-469-8590
mwahoske@tds.net

Secretary
Kim Hoppe
Coverys
262-271-0737
khoppe@coverys.com

Treasurer
Judith Cranberg
Froedtert Hospital
414-805-2645
jcranber@fmlh.edu

Board Members
Nancy Duran
Aurora Health Care
414-313-3821
nduran37@yahoo.com

Michelle Lahey Reed
Froedtert Hospital
262-257-3018
michelle.reed@froedtert.com

Sheridan Ryan
Medical College of Wisconsin
414-955-3153
sryan@mcw.edu

Sandy Somsen
Baldwin Area Medical Center
715-684-6762
sandy.somsen@healthybaldwin.org
Newsletter Chair

Karen Whyms
Aurora Health Care
karen.whyms@aurora.org

Risky Business is a publication of the Wisconsin Society for Healthcare Risk Management (WSHRM), a chapter of the American Society of Healthcare Risk Management. It is distributed to WSHRM members with information pertinent to the field of risk management.

Address all questions and comments to Editor:
Sandy Somsen
715-684-6762
sandy.somsen@healthybaldwin.org

Board Notes

Board Meeting Schedule
WSHRM Members are encouraged to attend board meetings. If you have an agenda item, please contact a Board member. The meeting schedule is shown on the WSHRM website.

Interested in a Board Position?
Anyone with questions about volunteering for a position with the WSHRM Board, please contact Kyle Fromm at kyleafromm@bluecrossmn.com.

Potential Sponsors
If your organization is interested in being a sponsor at one of WSHRM's educational programs, please contact Patti Erickson at patti.erickson@wfhc.com.

Planning Committee Volunteers
If you are interested in serving on WSHRM Conference Planning Committee, contact Patti Erickson at patti.erickson@wfhc.com.