JONES WALKER

e*bulletin

HEALTH CARE

June 2010 Vol. 4 healthcare@joneswalker.com

IN THIS ISSUE:

HIPAA TRAINING: AN OFTEN UNDERUTILIZED TOOL IN AN ORGANIZATION'S EFFORT TO PREVENT BREACHES

On February 17, 2009, the Health Information Technology For Economic and Clinical Health Act, also known as the "HITECH Act," was signed into law. The HITECH Act was one of the provisions contained in President Obama's American Recovery and Reinvestment Act (ARRA), which in addition to describing Federal initiatives designed to encourage the use of health information technology, made some significant changes to the existing Privacy and Security Regulations that are a part of the Health Insurance Portability and Accountability Act or "HIPAA." These changes, many of which became effective in February 2010, include new rules regarding an individual's right to receive an accounting of disclosures of their protected health information (PHI), provisions regarding business associate accountability and liability, and new limitations on the use and disclosure of PHI. The HITECH Act strengthened HIPAA's enforcement provisions, by, among other things, giving State attorneys general the right to bring civil actions in federal courts for violations of the privacy and security rules, and also increased HIPAA's penalty provisions by creating a tiered penalty approach to violations, such that the more severe the violation, the higher the penalty. For example, whereas prior to the passage of the HITECH Act, the U.S. Department of Health and Human Services (HHS) could have imposed a fine of not more than $25,000 per entity per calendar year, penalties now can be as high as $1.5 million per entity per calendar year.

Perhaps the most extensive changes contained in the HITECH Act are those concerning breach notification requirements. Specifically, if a suspected breach of unsecured PHI occurs, a facility must investigate the breach to determine whether it involved an impermissible use or disclosure of PHI that violates HIPAA and does not fall within an exception, and must also determine if the impermissible use or disclosure poses a significant risk of financial, reputational, or other harm to affected individual(s). Generally, if a facility determines that a breach of unsecured PHI has occurred (and none of the exceptions apply), written notice must be provided to individuals whose PHI may have been accessed. To the extent possible, the notice must briefly describe what occurred, including the date of the breach and the date of the discovery of the breach, if known; the types of unsecured PHI that were involved; what steps the affected individual(s) should take to protect themselves from potential harm resulting from the breach; what the facility is doing to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and must provide contact procedures for individuals to ask questions or learn additional information, which must include a toll-free number and e-mail address,

website, or postal address. If more than 500 individuals are affected by the breach, notice must also be sent to the media, as well as to HHS, which will post the notice on its website. The notifications must occur within 60 days of when the breach was or should have been reasonably discovered.

It is clear that the changes made to HIPAA by the HITECH Act are designed to ensure that entities take all necessary steps to comply with the privacy and security rules. In addition to the financial impact of paying potential penalties, organizations must expend significant amounts on the investigation and remediation of breaches, as well as on complying with the HITECH Act's breach notification provisions. Yet despite the potentially significant financial burden that may result from a breach of unprotected health information, a recent collaborative survey of 220 hospitals across 43 states conducted by Identity Force and the American Hospital Association revealed that 41.5 percent of the hospitals had 10 or more data breaches per year. In addition, as of May 1, 2010, the U.S. Department of Health and Human Services listed 32 organizations that had reported breaches of unsecured protected health information affecting 500 or more individuals since January 1, 2010.

Another recent survey of 250 hospital executives, conducted by HIMSS Analytics, found that two-thirds of those reporting breaches indicated that the breaches were attributable to unauthorized access to information by employees. The survey also revealed that 79 percent of the respondents indicated that they had provided increased training for employees as a result of the breaches.

While many entities are no doubt working to ensure compliance with the HITECH Act's requirements and are attempting to put into place breach reporting plans, perhaps the best way to address potential breaches of protected health information is to minimize the likelihood of them occurring in the first place. An often-underutilized tool available to entities seeking to minimize breaches is the implementation of an effective, recurring organization-wide training program. Despite the fact that training has been required by HIPAA for years, there may be a need to evaluate the effectiveness of existing training programs and perhaps to restructure them. For example, the Identity Force study revealed that 37.9 percent of the respondents either did not have training programs regarding the misuse of individual identification, or they indicated that although they had such training programs, very few employees had been trained. Similarly, a 2009 study of 77 healthcare facilities conducted by the Ponemon Institute indicated that only 53 percent of respondents reported that their organizations provide adequate staff training, while 47 percent of respondents reported that staff training was inadequate.

The reality of the situation is that workforce training can greatly help organizations reduce or even prevent HIPAA violations, including breaches of unsecured PHI. If an entity’s staff does not have a full understanding of an organization’s HIPAA policies and procedures, how HIPAA violations and security breaches occur and what they can do to prevent them, then violations of the privacy and security requirements would likely be more apt to occur.

So, organizations should start now to evaluate, redesign and/or implement training programs that effectively communicate privacy and security requirements. Rather than providing a “one-size-fits-all” program, training should be customized to fit the roles and responsibilities of the staff. Cookie-cutter training is less likely to be effective than training that takes into account the specific privacy issues that different staff is likely to encounter. A training program for nurses, for example, may look very different from a training program for financial service coordinators. Training may be more or less

intensive, depending on how likely it is for a breach to occur and how harmful the effects of any such breach would likely be.

Training should be interactive. Active learning is often more effective than passive learning. Real-life examples or hypothetical examples utilizing real processes and challenges can help staff relate to the privacy issues that can occur on any given day. Training should be on-going. Annual training is essential, but should be supplemented with frequent updates. The updates can be sent via email and can also be posted in common areas. They should be relatively brief and are most effective when they discuss timely privacy issues. For example, on April 27, 2010, the United States Attorney for the Central District of California issued a press release indicating that an ex-UCLA healthcare employee was sentenced to four months in federal prison for violating HIPAA by accessing private and confidential medical records, mostly of celebrities and other high-profile patients. This case would be a perfect opportunity to disseminate an email briefly discussing the case, as well as the issues involved in the unauthorized accessing of medical records. In short, it represents a "teachable moment," a real-life example that can illustrate how easily HIPAA can be violated and the potential penalty of doing so.

Teachable moments should also be incorporated into interactive training sessions and can be utilized to illustrate the complexities of analyzing HIPAA violations. For example, Griffin Hospital in Derby Connecticut recently notified 957 patients of an apparent breach of PHI involving a former radiologist, who had been terminated from the Hospital's contracted radiology group and lost his medical staff privileges at the Hospital on or about February 2, 2010. Despite his termination and removal from the medical staff, for approximately one month thereafter, the radiologist continued to access patient radiology reports on the Hospital's PACS system utilizing the passwords of other radiologists and a radiology employee without their knowledge. The radiologist used the information he obtained from the PACS system to contact patients in order to persuade the patients to obtain services from him at another institution. This case is the perfect vehicle to discuss numerous HIPAA-related questions such as: What was the hospital's role in this breach of PHI? What could it have done to prevent it? What systems should it have in place to ensure the radiologist could not access the hospital's PACS system post-termination? How may the radiologist have obtained the passwords of other radiologists and what could the other radiologists have done to prevent the unauthorized use of their passwords? In short, the unfortunate situation at Griffin Hospital can lead to robust discussions and thoughtful analyses of the many complexities that may be involved when a breach of unsecured PHI occurs.

When designing or redesigning a training program, an organization must train its workforce members, including employees, volunteers, and trainees, as well as other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity. An organization should also consider extending its training to members of its medical staff (who generally do not fit into any of the forgoing categories). For example, in one recent case, after watching a TV news report at home, an Arkansas physician accessed a patient's medical record to determine if the news report were true. The physician admitted he had no legitimate purpose in accessing the patient's medical record and pled guilty to a violation of HIPAA. This demonstrates that including medical staff education in an organization's training program is something that should be seriously considered.

JONES WALKER

e*bulletin

HEALTH CARE

June 2010 Vol. 4 healthcare@joneswalker.com

An organization's commitment to creating, evaluating and/or redesigning a training program containing the elements described above will take resources—both time and money. However, for those who may worry that the cost of implementing highly effective organization-wide training may be higher than what is currently being spent on such training, it may be that a program restructuring may result only in a reallocation of existing dollars, which have already been earmarked for training. Furthermore, consider that the 2009 Ponemon Institute study reported that an organization's cost associated with a breach was an estimated $202 *per record breached*. This does not include the cost amount of any penalties that may also be incurred, and translates into a cost of over $1 million for a breach involving 5,000 records. Blue Cross Blue Shield of Tennessee announced at the beginning of this year that it had spent more than *$7 million* in responding to a theft of 57 hard drives containing the unencrypted personal and health data of close to one million of its current and former members. It appears this cost related only to Blue Cross' remediation efforts, including investigating the breach, strengthening existing security measures, restoring a back-up of the stolen hard drives, sending notification letters to those affected as well as to company and group administrators, and providing affected members with free credit monitoring for one year. When viewed it this context, most organizations would probably agree that shifting or allocating money into efforts to try to prevent HIPAA violations and breaches of unsecured PHI through the use of effective, recurring, organization-wide training—rather than into post-breach remediation, notifications, and penalties—is money well spent.

If you would like assistance in more fully understanding the HIPAA and HITECH Act requirements, or if you would like assistance in structuring or restructuring a HIPAA/HITECH training program, please contact Lynn M. Barrett.

Lynn M. Barrett
305.679.5712
lbarrett@joneswalker.com

JONES WALKER

e*bulletin

HEALTH CARE

June 2010 Vol. 4 healthcare@joneswalker.com

ARE YOU PROTECTED FROM MEDICARE SECONDARY PAYER LIABILITY?

Since the adoption of the Medicare Secondary Payer Act in 1980 (MSPA), the United States government has the right to claim reimbursement for Medicare expenses paid on behalf of an injured party from settlements, judgments, awards or other payments. However, this right of reimbursement was rarely, if ever, exercised because the law did not impose any duty to report payments made to a Medicare recipient. This changed radically in 2007 with the enactment of the Medicare, Medicaid, and SCHIP Extension Act of 2007 (MMSEA), which imposes onerous reporting requirements on third parties making payments to Medicare recipients, as well as significant liability for reimbursement and penalties for failure to protect Medicare's reimbursement interest.

The United States government has begun to exercise its rights to reimbursement of Medicare expenses with serious consequences for businesses, insurers, third party administrators, or anyone seeking to resolve the personal injury claims of present or future Medicare recipients.

Legislative History and Substance of Acts

A brief legislative history of the MMSEA is helpful in understanding the many dangers posed by this legislation. Prior to 1980, Medicare was a Primary Payer of medical expenses to eligible recipients (those 65 years of age and older, certain disabled people, and people suffering from end-stage renal disease). As a Primary Payer, Medicare was generally not entitled to reimbursement of medical expenses paid on behalf of injured tort victims.

In 1980, prompted by projections of rising Medicare deficits, Congress enacted the Medicare Secondary Payer Act (MSPA), making Medicare a Secondary Payer to such Primary Payers as group health insurers, liability insurers, self insurers, and workers' compensation systems. Medicare was authorized to conditionally pay medical expenses subject to reimbursement from later settlements, judgments, awards, or other payments. The MSPA also empowered the Centers for Medicare and Medicaid Services (CMMS) to pursue damages against any primarily responsible party. However, Medicare's right of reimbursement under the MSPA was almost universally ignored because there was no duty or mechanism to report payments by Primary Payers to Medicare beneficiaries and no penalties for failing to protect Medicare's interest.

In 2007, faced with mounting Medicare deficits, Congress attempted to close these reimbursement loopholes by enacting the Medicare, Medicaid, and SCHIP Extension Act (MMSEA). The MMSEA protects Medicare's reimbursement rights in personal injury cases in which the plaintiff is a Medicare beneficiary by imposing stringent reporting requirements and onerous liability for failing to ensure that Medicare is reimbursed.

The reporting requirements apply to anyone who is potentially liable to a Medicare beneficiary for payment of medical expenses. Such Responsible Reporting Entities (RREs) are required to register with CMMS for on-line reporting, to report any settlements or payments to the Medicare beneficiary and to ensure that Medicare is reimbursed within 60 days of any verdict or settlement. Reports are made through CMMS' contractor, the Coordinator of Benefits Contractor (COBC).

JONES WALKER
e*bulletin
HEALTH CARE

June 2010 Vol. 4 healthcare@joneswalker.com

Preliminary and final statements of the amount of reimbursement are obtained from the Medicare Secondary Payer Recovery Contractor (MSPRC). Payment is made to the CMMS.

The MMSEA imposes a $1,000.00/day/claim fine for late reporting. CMMS has a statutory lien and its own right of action for recovery against any RRE if reimbursement is not made. Medicare may sue any party responsible for reimbursement for double damages. Additionally, a private cause of action for double damages was created allowing the parties or any citizen to enforce the reimbursement obligation. Finally, CMMS may penalize a beneficiary by rejection of future benefits if Medicare is not reimbursed.

Medicare Reimbursement Procedure

Due to the reporting requirements and the time needed to obtain a final demand from the MSPRC, it is imperative that the process for determining the amount of reimbursement be initiated as early in the proceedings as possible. The following describes the procedure involved:

1. RRE is initially placed on notice of claim by a potential Medicare beneficiary.
2. RRE obtains a "Consent to Release Form" and additional information from beneficiary including:
    - Name
    - Social Security number and/or Health Insurance Claim Number
    - Date of birth
    - Gender
3. RRE sends correspondence to COBC notifying it of the:
    - Claim
    - Potential that the RRE has primary responsibility
    - Beneficiary's personal information
    - Date of injury
    - ICD-9 codes applicable to the injury
4. Medicare creates electronic record of claim and notifies MSPRC within 14 days.
5. MSPRC sends a "Rights and Responsibilities Letter" to the beneficiary, beneficiary's attorney, and any RRE that has provided a "Consent to Release Form" regarding the obligation to reimburse Medicare.
6. MSPRC compiles information regarding conditional Medicare payments made to the beneficiary related to injury.

7. On request but no sooner than 65 days from the "Rights and Responsibilities Letter," MSPRC issues a "Conditional Payment Letter," setting out by ICD-9 codes the treatment related to the injury and an initial estimate of the amount owed to Medicare.
8. The beneficiary and RREs review the "Conditional Payment Letter" letter by ICD-9 codes for relatedness to injury. Beneficiary strikes out any ICD-9 codes he believes are unrelated to the accident and sends the "Conditional Payment Letter" back to MSPRC along with along with an explanation for any deleted ICD-9 codes.
9. MSPRC sends an "Amended Conditional Payment Letter," stating its final determination of the ICD-9 codes related to the injury.
10. Beneficiary and RRE either conclude settlement or proceed to verdict after trial.
11. The executed release or judgment is sent to MSPRC with a request for a "Final Payment Letter" and any payment instructions.
12. Within 14 days, MSPRC issues a "Final Demand Letter," containing Medicare's final lien amount to be paid.

Future Medicare Payments

Claimants for whom Medicare may incur a liability to pay medical expenses in the future pose a significant problem because the MMSEA does not set forth any procedure for determining the amount to be set aside for payment of future medical expenses or the manner in which it should be set aside. Most commentators believe that the beneficiary and the MSPRC should agree to an amount to be set aside for future medical payments to be placed in an account administered by the claimant's attorney or a third party. Failure to make arrangements to fund future medical liability could result in Medicare denying benefits for any future medical expenses.

Conclusion

The MMSEA sets up a lengthy, complex process for determining Medicare's reimbursement rights and imposes significant liability for the failure to follow it. The United States government has demonstrated that it intends to pursue Medicare reimbursement even for relatively small amounts. Thus far, it has sought to hold the beneficiary, beneficiary's attorney, the paying defendant, and the defendant's insurers liable for reimbursement and penalties.

Compliance with the MMSEA requires early identification of claimants who are or may become Medicare beneficiaries and a formal program to obtain the necessary information, Consent to Release and a determination of the final amount to be paid to Medicare. When litigation is involved, defense counsel should attempt to work with beneficiary's counsel to comply with the MMSEA. If the beneficiary's counsel fails to cooperate, defense counsel should be prepared to inform the court of the situation and obtain necessary orders requiring compliance.

The MMSEA has no "safe harbor" provisions. Liability for reimbursement and penalties can be avoided only by strict compliance. Leaving compliance to the beneficiary's attorney is not sufficient even if the beneficiary's attorney agrees to comply with the MMSEA and agrees to indemnify the defendant.

If you currently do not have a program to comply with the MMSEA or are concerned about the adequacy of your program, Jones Walker has attorneys available to assist you. Any questions concerning the issues raised herein can be addressed by either of the authors.

William L. Schuette
225.248.2056
wschuette@joneswalker.com

Kevin O. Ainsworth
225.248.2036
kainsworth@joneswalker.com

JONES WALKER

e*bulletin

HEALTH CARE

June 2010 Vol. 4 healthcare@joneswalker.com

JONES WALKER PRESENTS
HEALTH CARE SEMINARS AND WEBINAR SERIES

Jones Walker will present two health care seminars: **September 14, 2010**, in Baton Rouge, Louisiana, and **September 24, 2010**, in Fort Lauderdale, Florida. In addition, Jones Walker will present a series of six free monthly webinars. Each webinar will feature presentations from attorneys experienced in the pertinent areas.

The webinars will cover the following topics:

- **July 27, 2010**: **"False Claims Act and Internal Investigations"**
  Donald W. Washington
- **August 5, 2010**: **"Key Issues and Updates from the Health Care Reform Legislation"**
  Myla R. Reizen, Lynn M. Barrett, and Neely Sharp Griffith
- **August 12, 2010**: **"RAC/CERT/Government Data Mining & Billing Compliance"**
  Myla R. Reizen
- **August 19, 2010**: **"HIPAA and HITECH Compliance—The Reality for Health Care Providers in 2010"**
  Lynn M. Barrett
- Date TBD: **"Health Care Transactions—What You Need To Know"**
  Allison C. Bell
- Date TBD: **"Tax Implications for Health Care Providers"**
  Rudolph R. Ramelli

The initial webinar of the series will be held Tuesday, July 27, 2010.

For more information on either of the seminars or the webinar series, or to register for any of these programs, please contact **Courtney Farley** at 504.582.8121, or e-mail her directly by clicking here. Once registered, you will receive webinar participation instructions and login information at least one day before the event.

JONES WALKER

e*bulletin

HEALTH CARE

June 2010 Vol. 4 healthcare@joneswalker.com

Jones Walker offers a broad range of legal services to health care industry clients, including regulatory compliance, litigation, investigations, operations, and transactional matters. These legal principles may change and vary widely in their application to specific factual circumstances. You should consult with counsel about your individual circumstances. For further information regarding these issues, contact:

Myla R. Reizen
305.679.5716
mreizen@joneswalker.com

Health Care Attorneys

A.G. "Alec" Alexander, III
Lynn M. Barrett
Allison C. Bell
Amy C. Cowley
Mark A. Cunningham
Nadia de la Houssaye
Mollye M. Demosthenidy
Neely S. Griffith
Pauline F. Hardin
Kathleen A. Harrison
John J. Jaskot
Jonathan R. Katz
Joseph J. Lowenthal, Jr.
Hugh C. Nickson, III
Rudolph R. Ramelli
Myla R. Reizen
Gary J. Russo
Donald W. Washington
Amy M. Winters

This newsletter should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult your own attorney concerning your own situation and any specific legal questions you may have.

To subscribe to other E*Bulletins, visit http://www.joneswalker.com/ecommunications.html.