

HIPAA Breach Notification Rule Issued By HHS: Compliance Date Is Fast Approaching

by Diane Kutzko

Introduction

On August 24, 2009, the Department of Human Services (HHS) issued regulations (the Interim Final Rule) concerning covered entities' HIPAA obligations under the HITECH Act to notify patients of breaches of the privacy and security of protected health information (PHI). The Rule becomes effective September 23, 2009 and public comment is open until October 23, 2009. The Department of Human Services has stated that it will not enforce the Rule (i.e., impose penalties) until February 22, 2010. As a practical matter, this provides some time to determine what needs to be done to comply and to put policies and procedures in place. However, because the Rule does state that it *applies* thirty days from the publication date (i.e., September 23, 2009), covered entities should begin to consider what they need to do to update their policies and procedures as soon as possible.

What is the scope of the Rule?

As a threshold matter, the rule applies only to "unsecured PHI," whether it is maintained in electronic or paper form, or communicated orally. "Unsecured PHI" means protected health information that "has *not* been rendered unusable, unreadable or indecipherable" consistent with an April 2009 Guidance from HHS. Those standards for encryption and destruction can be found at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html. Entities that secure health information as specified by HHS are relieved from having to notify in the event of a breach of such information.

Under the original HIPAA Security Rule, encryption was an "addressable" standard, i.e., it was optional and not required. Providers who made a decision to encrypt electronic PHI (E PHI) at that time will need to check to make sure that the technologies used were

(continue next page)

For Your Information

- As we previously communicated, the FTC announced on July 29th that it will delay enforcement of the Red Flags Rule until November 1, 2009 and make adjustments to assist low-risk entities with compliance. For further information call or e-mail Tricia Hoffman-Simanek, 319-365-9461; psh@shuttleworthlaw.com
- Shuttleworth lawyers, Diane Kutzko and Nancy Penner, will be speakers at a continuing education seminar sponsored by Lorman Education Services entitled "Medical Records Law in Iowa" on November 3, 2009 in Cedar Rapids. Please visit www.lorman.com/ID385079 to view the seminar details. If you are interested in more information, contact Diane at dhk@shuttleworthlaw.com or Nancy at njp@shuttleworthlaw.com or call them at 319-365-9461. Lorman is pleased to offer a \$50 discount off the fee for this seminar. Please mention discount code Z7745121 when registering.
- Special thanks to Shuttleworth summer associates and University of Iowa law students, Cindy Boyle and Jennifer Hennessy, for contributing to this issue.

ALSO IN THIS ISSUE

**Reporting requirements
when resolving claims**

Page 3

New case on EMTALA

Page 5

**New case on Peer
Review**

Page 7

(Cont. from Page 1) . . . HIPAA Breach Notification Rule

consistent with the HHS Guidance. Providers who made a determination not to encrypt in order to secure PHI at that time may wish to revisit this issue, because if EPHI is encrypted consistent with HHS standards, there is *no* duty to notify in the event of a breach. In addition, there is no duty to notify in the event of a breach incident involving PHI in paper form if it is shredded or otherwise destroyed consistent with the HHS Guidance.

When does a breach occur?

As clarified by the Rule, under the HITECH Act, a breach is defined as the “unauthorized acquisition, access, use or disclosure of protected health information in a manner not permitted under the [Privacy Rule] which compromises the security or privacy of the protected health information.” Not all such acquisition, access, use or disclosure is a breach that requires notification.

The first step in determining if a breach has occurred is to determine whether there has been a use or disclosure of PHI that violates the Privacy Rule. If such a use or disclosure has occurred, the next step is to determine whether such a use or disclosure compromises the security or privacy of the PHI. Under the Rule, HHS has clarified that PHI is compromised only if it poses a significant risk of financial, reputational or other harm to the individual. Therefore there is a “harm threshold” that needs to be overcome in order for a breach to require notification, even if a breach occurred. If there was little risk of such harm, no notification is necessary.

The next step: Risk assessment

To determine whether there has been a significant risk of harm, covered entities (and their business associates) are required to perform a fact-specific risk assessment, taking into account the following:

- Who impermissibly used and/or received the PHI?
- Were immediate mitigating steps taken and did they eliminate or reduce the risk of harm to the individual, e.g., was the PHI returned prior to being accessed improperly?
- What was the type and amount of the PHI involved in the improper use or disclosure?

Exceptions to the definition of breach

The Rule also clarifies exceptions to the definition of breach, i.e., notification is not required in the following circumstances:

- Unintentional use by an employee or entity of the disclosing covered entity – must be by a member of

the workforce or individual acting “under the authority of the covered entity or business associate” and who used the PHI “in good faith” and within the scope of his or her employment or professional relationship. *In addition*, the unintentional use cannot result in further use or disclosure.

- Inadvertent disclosures to similarly situated individuals within the same facility – under the Rule, this is expanded to disclosures within the same covered entity, business associate or organized health care arrangement. Also, two persons are “similarly situated” if they are both authorized to access PHI, even if they are not authorized to access the same types of PHI. There cannot be further use or disclosure that violates the Privacy Rule.
- Circumstances under which the unauthorized recipient cannot reasonably be expected to be able to retain it. This applies if the covered entity or business associate has a “good faith belief” that the recipient could not reasonably have been able to retain the PHI.

In addition, there is an exception if the unsecured PHI is a limited data set – i.e., one that does not contain 16 direct identifiers specified in the HIPAA Privacy Rule and also excludes birth dates and zip code information.

When a breach occurs, what are the notice requirements?

An entity may take a “reasonable amount of time” to determine whether an impermissible use or disclosure constitutes a breach requiring notification. *However*, the time for notification—which is sixty days—runs from the discovery of the unauthorized use or disclosure, rather than from the time the assessment is completed. The obligations are as follows:

- As a general rule, a covered entity must notify every individual whose unsecured PHI has been “breached,” i.e., every patient for whom an unauthorized use or disclosure poses a significant risk of financial, reputational or other harm. Other unauthorized uses or disclosures do not require notification. The covered entity makes this determination based on the risk assessment described above.
- Knowledge of any member of the workforce is attributed to the covered entity; the Rule encourages covered entities to implement reasonable systems for detecting breaches.

(continue next page)

(Cont. from Page 2) . . . HIPAA Breach

- Notice must be sent no later than *sixty days* after the covered entity first discovers the breach (unless law enforcement requests a delay) – but if the covered entity could reasonably conclude its investigation and send notice prior to 60 days, it may not be appropriate to allow the entire sixty days to run.
- The notice must include, to the extent possible, a description of what happened, including the date of the breach; a description of the unsecured PHI; recommended steps for individuals to take to mitigate potential harm; and a description of what the covered entity is doing in response; and contact information.
- In the event that the breach involves PHI from 500 or more individuals, the covered entity must notify the Secretary of HHS at the same time it notifies the affected individuals.
- If the breach involves more than 500 patients in one state, “prominent” media outlets in the geographic area must be notified.
- Note: in cases of less than 500 affected individuals, the covered entity must keep a log of any breaches and submit the log to the Secretary within sixty days of the end of each calendar year.■

Getting ready: What you need to do

If you use and disclose *unsecured* PHI, it is important that you implement policies and procedures, covering the following: (1) education and training members of your workforce (includes employees, independent contractors, and volunteers) to detect and report breaches; (2) investigation and risk assessment to determine whether an unauthorized use or disclosure constitutes a breach which requires notice; (3) notice to patients and others as required by the rule. In addition, business associate agreements may need to be amended as well as your notice of privacy practices to inform patients with regard to their rights following a breach. While the enforcement for the Rule is February 22, 2009, the effective date is September 23, 2009, and therefore you should be working on these issues as soon as possible. As a possible first step prior to September 23, you may wish to consider a memo to members of your workforce concerning their obligation to report any unauthorized uses or disclosures of PHI that they are aware of to someone you designate (whether that be the Privacy or Security Officer, or risk manager). Any reported unauthorized uses and disclosures could then be investigated and assessed, even before formal policies and procedures are in place. In addition, you may wish to communicate to your business associates reminding them of their obligation to report any breaches to you immediately.

As it did with the Privacy Rule and Security Rule, Shuttleworth & Ingersoll is happy to assist you with policies, procedures, forms, and form letters, as well as employee training. Please contact Diane Kutzko, dhk@shuttleworthlaw.com, for further information.■

Reporting requirements when resolving claims or lawsuits with Medicare recipients take effect January 1, 2010 but affect resolutions after July 1, 2009

by Cindy Boyle and Tricia Hoffman-Simanek

On December 29, 2007 former President George W. Bush signed the Medicare, Medicaid, and SCHIP Extension Act of 2007 (MMSEA). The purpose of § 111 of the Act is to protect Medicare’s interest in beneficiaries’ claims against third parties for medical expenses. Claims against third parties arise in the context of liability insurance, no fault insurance, and workers’ compensation. Section 111 provides mandatory requirements where Medicare is the secondary payer.

In an effort to protect Medicare’s interest, the Act sets

forth reporting requirements for responsible reporting entities (RREs). **An RRE is any entity that pays a settlement, judgment, award, or other payment on a claim to a Medicare recipient or an individual who is eligible for Medicare benefits (as future medical expenses may be an issue).** This includes insurers and self-insured entities. Any entity that is responsible for the assumption of risk and medical claim liabilities of another is an RRE. Providers with traditional insurance should coordinate with their carrier on compliance issues.

(continue next page)

(Cont. from Page 3) . . . Reporting requirements when resolving claims or lawsuits

Medicare will use the additional information obtained through the reporting to cut costs in two ways. First, Medicare will be able to determine when it is appropriate to refuse to pay medical bills because there is another primary responsible party. Second, Medicare will be able to identify instances where it is entitled to reimbursement because a beneficiary has recovered twice, both from Medicare and from a claim against an insurer or self-insured.

Requirements Under the MMSEA

Under the Act, an RRE had to register with the CMS coordinator of benefits contractor by June 30, 2009. Beginning on January 1, 2010, RREs are required to report to CMS any settlement, award, judgment or other payment(s) made to a Medicare beneficiary. **However, the January 1, 2010 report MUST INCLUDE all settlements, awards, judgments, etc., made on or after July 1, 2009.** These disclosures should be made as part of a quarterly report to CMS.

The RRE is solely responsible for determining whether an individual is a Medicare beneficiary or eligible for benefits. It is not a defense that the RRE did not know that an individual was receiving Medicare benefits. The individual receiving Medicare does not have a similar duty to report to CMS.

An RRE must report a settlement to CMS regardless of whether there is an admission or determination of guilt. Likewise, the RRE must report whether there has been a full or partial settlement. There is a limited exception to the reporting requirement where the amount of the claim is very small. Until December 31, 2010, an RRE does not need to report any one-time settlements of less than \$5,000. This threshold amount is reduced to \$2,000 for 2011 and \$600 for 2012.

Failure to Meet Reporting Requirements

If an RRE fails to meet the reporting requirements under the MMSEA, the RRE may be subject to fines or penalties. The fine for failure to meet the requirements is \$1,000 per day, per claim that has the RRE has failed to properly report.

In addition to fines and penalties, the RRE may also be subject to a private cause of action if the RRE refuses to reimburse Medicare or make a necessary primary payment. The government can sue the RRE to recover any amounts due. A Medicare beneficiary

can also sue the RRE for damages if the individual's Medicare benefits are suspended because the RRE failed to make necessary payments.

Anyone involved in a settlement with a Medicare beneficiary, including the plaintiff's attorneys, defendant's attorneys, insurance carriers, self-insureds, and third-party administrators may be liable.

What Should RREs Do?

The first step for RREs is to register with CMS. RREs can contact an agent to handle this step, but the RRE is still responsible for the agent's failure to comply with any of the MMSEA requirements. After the RRE registers with CMS, CMS will create an RRE file and send the reporting ID and quarterly reporting deadline information to the RRE.

As RREs continue working on claims brought prior to the enactment of the MMSEA and begin working with new claimants, the RREs should identify which claimants are Medicare beneficiaries or Medicare-eligible. The RRE should obtain the individual's personal information, including social security number and date of birth and conduct their own determination of whether the individual is a Medicare beneficiary or Medicare-eligible. The RRE should not rely on representations by the individual as the RRE is still liable even if the RRE relies on a statement by the claimant that he/she is not a Medicare beneficiary. Instead, a CMS program allows RREs to use this information to query whether a claimant is a beneficiary by submitting a list of new claimants to CMS once each month. CMS will return a report to the RRE indicating whether the individuals listed are Medicare beneficiaries or not. If a claimant is a Medicare beneficiary, CMS will provide additional information including an ID number to use in further filings relating to that claimant.

Do note that RREs are not exempt from meeting privacy requirements and must invest resources to ensure that claimants' personal information is protected. However, the RRE does not need to obtain approval from the beneficiary claimant prior to making this disclosure. An important part of giving CMS notice is providing the appropriate ICD-9 codes that describe the claimant's injuries.

Before making a settlement the RRE should take into consideration the amount of Medicare liens (and

(continue next page)

(Cont. from Page 4) . . . Reporting requirements when resolving claims or lawsuits

potential for future liens). The RRE should either request the interim Medicare payment statements from the claimant or obtain the claimant's consent to request the interim statements directly from CMS.

RREs should also obtain a final reimbursement demand letter from Medicare before finalizing settlement. RREs should also be aware that it is risky to distribute a settlement before receiving the final reimbursement demand letter from CMS. If the RRE settles with the claimant before ensuring that all Medicare liens have been paid, the RRE can still be liable to Medicare for the additional amounts due.

CMS recommends that for each liability claim, the RRE should perform a query with CMS at least two times: (1) at the time the claim is filed; and (2) at the time settlement discussions begin or a settlement is reached. In workers' compensation, a query should be done each time a payment/installment is to be made.

Implications

One of the biggest implications of the Act is that it will cause substantial delay in settlements involving a Medicare beneficiary. The reporting requirements will require RREs to invest additional time and resources into organizing settlements. Because settlement does

not preclude future liability to CMS, insurers or self-insureds will often be hesitant to settle until they have received a final demand notice from CMS indicating the exact amount due. There are currently no time requirements for the CMS demand notices, and it could take months or even over a year to receive a final demand letter from CMS once the RRE has reported the settlement.

Additionally, because a claimant is not always required to provide personal information that is necessary for an RRE to begin reporting at the outset of discussions relating to a claim, a reluctant claimant can slow down process even further.

Another big implication of the Act is that it takes away much of the finality that RREs previously could achieve through settlements. Under the Act an RRE may still be subject to fines and penalties, additional reimbursements of CMS, additional post-treatment Medicare costs, and private causes of action even after the RRE has reached a final settlement agreement with the claimant.

It should also be noted that CMS is not bound by any allocation by the parties to "medical expenses" – even when the court has approved such an allocation. ■



An Iowa U.S. District Court determines that an EMTALA transfer form did not protect a hospital from EMTALA liability

by Jennifer Hennessy and Nancy Penner

On May 14, 2009, the U.S. District Court for the Northern District of Iowa published an opinion involving the effect of a completed transfer form under the Emergency Medical Treatment and Active Labor Act ("EMTALA"). *Heimlicher v. Steele*, 615 F.Supp.2d 884 (N.D. Iowa 2009) involved an EMTALA claim against a hospital as well as claims of negligence against the hospital and an emergency room physician. The case arose out of the transfer of a labor patient to another hospital 100 miles away and the death of the baby, delivered by C-section at the receiving hospital.

The court described the facts to

include the following: The patient was 34 weeks pregnant when she arrived at a hospital experiencing bleeding, pain in her abdomen, and contractions. The ER physician ruled out the possibility of a placental abruption, a serious condition where the placental lining separates from the uterine wall. An ultrasound technician sent the images to the on-call radiologist who communicated a diagnosis of "mass vs hemorrhage vs fibroid." The ER physician testified he did not recall receiving this information. The ER physician spoke to an obstetrician at a larger hospital and told him that the patient's placenta was not abructing, her uterus was not rup-

tured, and her condition was stable. The obstetrician agreed to accept the transfer based on this information. The patient, accompanied by a nurse, was transferred to the larger hospital by ground ambulance as the weather prevented air transport. Upon leaving the first hospital, the patient almost immediately began having rapid contractions, severe abdominal pain, and profuse bleeding. Fetal monitoring indicated the baby was in distress. The patient's condition was not reported and the ambulance apparently passed nearby other hospitals which could have performed a C-section. The obstetrician performed

(continue next page)

(Cont. from Page 5) . . . EMTALA transfer forms

an immediate C-section when the patient arrived at the larger hospital but the baby was stillborn. It was not disputed that the cause of death was a placental abruption or that the baby likely could have been delivered without complications if a C-section had been performed at the first hospital (which was equipped and staffed to do C-sections).

The verdict. The jury returned a verdict for the patient and against the ER physician and hospital on the negligence claim and against the hospital on the patient's EMTALA claim. The jury awarded approximately 1.7 million dollars in damages and on the negligence claim found the hospital was 70% at fault and the ER physician was 30% at fault.

The transfer form issue. There were many issues in the long published opinion, only one of which is discussed here—the impact of the completed transfer form on the EMTALA claim.

Under the facts of the case, the court found that the only way the first hospital was justified in transferring the patient was if:

- 1) her emergency medical condition was stabilized;
- 2) her condition was not stabilized but she requested transfer; or
- 3) her condition was not stabilized but the physician signed a certificate that the “medical benefits reasonably expected from medical treatment at another hospital outweighed the increased risks to her and her unborn child from the transfer.”

As to Number 1 above, the ER physician marked the transfer form

to indicate the patient had been stabilized, but the court found the certification “both curious and troublesome.” In addition to evidence that the patient was actually not stabilized, the physician went on to complete that part of the transfer form for *unstabilized* patients. In other words the form was not completed correctly. The court affirmed the jury finding that the patient had not been stabilized.

As to Number 2 above, even though the patient signed a consent to the transfer, the court found this did not amount to a request for a transfer.

As to Number 3 above, the hospi-

EMTALA transfer forms are important—but they are not guarantees against EMTALA liability.

tal argued that the ER physician's certification that the benefits outweighed the risks meant the hospital had no EMTALA liability. The court disagreed and found that there was evidence that the ER physician “signed the form without actually deliberating and weighing the medical risks and benefits of the transfer [and he] over-valued minimal or insignificant benefits, and he ignored serious foreseeable risks.” The court stated that “This invalidates his certification.” It is important to note that the ER physician was considered to be acting on behalf of the Hospital.

What does this case mean? EMTALA transfer forms are important—but they are not guarantees

against EMTALA liability. Under the ruling in this case, a completed transfer form with a physician certification is not enough to defeat an EMTALA claim. Instead, a jury will be allowed to consider whether an appropriate and reasonable risk/benefit analysis was made regardless of what a physician may or may not have documented on the transfer form. (To some extent, this is similar to informed consent forms. Completed informed consent forms are important and are definitely valuable in defending against a lack-of-informed-consent claim—but they do not necessarily provide guarantees against liability.)

The case also illustrates that—even though forms do not provide guarantees—it is still important that they be completed correctly. The ER physician in this case marked the patient was stabilized but then completed the section of the form that is only to be completed for unstabilized patients. This did not help. It is possible that the form itself was somewhat confusing, leading to this error.

In sum, the case teaches that EMTALA transfer forms are important—they will not be ignored and should be completed with care—but even a perfectly completed form will not protect a hospital from an EMTALA claim if a jury finds the actual transfer was problematic.

An important caveat. The results of any given case depend, in large part, on the facts of that case. It is clear that the *Heimlicher v. Steele* case was complicated in many respects. In a different case with different facts and proceedings, the outcome could be different. ■

Iowa Court of Appeals holds that a physician's credentialing file is protected peer review

by Nancy Penner

Iowa, like most states, has a specific statute (Iowa Code §147.135(2)) that protects the confidentiality of "peer review records." This is called the "peer review privilege." The purpose of the privilege is to protect the process and records in order to encourage candid and effective peer review.

People often think of peer review narrowly as only including a review of a specific case with a bad outcome or of a provider with a string of bad outcomes. However Iowa's statutory language is quite broad. It generally refers to peer review as the evaluation of services or competency.

The privilege therefore protects far more than what many assume.

In the context of a hospital and a physician, a credentialing file typically includes the physician's application and reapplications for membership to the medical staff, supporting documents and information, and the results of on-going quality review on the physician. In short, the material in a physician's credentialing file is compiled so that other physicians may evaluate the physician before granting or renewing privileges.

Plaintiffs in lawsuits against physicians and hospitals sometimes request a copy of the physician's credentialing file during the discovery phase of the lawsuit. Physicians and hospitals generally object to the request on the grounds that credentialing files are protected under Iowa's peer review privilege. Until May of this year, the Iowa appellate courts had not decided whether a credentialing file fell under the peer review privilege.

On May 29, 2009, in *Day v. Finley Hospital*, 2009 WL 1492661 (Iowa Ct. App 2009), the Iowa Court of Appeals decided this issue in favor of the hospital and held that a credentialing file was protected under Iowa's peer review statute. Even though *Day* was a negligent credentialing case in which the plaintiff was attempting to establish the hospital negligently credentialed a podiatrist, the Court still held the file was off-limits. The Court stated: "The legislature has spoken and has directed that peer review files be kept confidential, even when requested in litigation."

"The legislature has spoken and has directed that peer review files be kept confidential, even when requested in litigation."

The Court in *Day* specifically rejected an argument that the privilege should only protect records generated by the peer review committee and not documents gathered as part of the credentialing process. Instead, the Court held information could be protected by the statute "whether the information was generated by the peer review committee or not."

The Iowa decision in *Day* is important to hospitals, offices, physicians, and other providers. It is a positive step in keeping peer review records confidential and in encouraging effective evaluations. Hospitals and offices should consider whether their policies and practices take full advantage of Iowa's broad peer review privilege.

The hospital in *Day v. Finley Hospital* was represented by Connie Alt, Mark Zaiger, and Nancy Penner of Shuttleworth. The case was tried in Dubuque in December 2007 and the jury returned a verdict in favor of the hospital. ■

Contact us at:

Shuttleworth & Ingersoll, P.L.C.
115 Third St. SE, Suite 500
P.O. Box 2107
Cedar Rapids, Iowa 52406-2107
Phone: 319-365-9461
Fax: 319-365-8564

Health Law Practice Chair:

Diane Kutzko
dhk@shuttleworthlaw.com

For more information about Shuttleworth & Ingersoll, its Health Law Practice Group, and the attorneys who practice in health law, please visit our web site at:

www.shuttleworthlaw.com

This newsletter is intended for distribution to Shuttleworth & Ingersoll clients and to others who ask to be on the distribution list. If you wish to be removed from the distribution list, please contact Diane Kutzko or Nancy Penner (njp@shuttleworthlaw.com).

This newsletter provides general information only and should not be construed as legal advice. You should not act in reliance upon the information contained in this newsletter without consulting an attorney about your specific situation.