April 2013

p.s.

SCRIPTS

Legal updates for the health care community from Poyner Spruill LLP

Poyner Spruill LLP
ATTORNEYS AT LAW

WWW.POYNERSPRUILL.COM

INSIDE THIS ISSUE

p.s. This inaugural issue of *Scripts* is the **only copy we will issue in print.** If you would like to receive future issues of *Scripts*, sign up on our website, www.poynerspruill.com, and click on sign up for alerts at the top of the page.

Key Provisions In the Final Omnibus HIPAA/ HITECH Rules and What They Mean for You

By Elizabeth Johnson

On January 25, 2013, the U.S. Department of Health and Human Services (HHS) published omnibus final regulations modifying the HIPAA Privacy, Security, Breach Notification and Enforcement Rules. The modifications implement most of the privacy and security provisions of the HITECH Act and relevant provisions of the Genetic Information Nondiscrimination Act. While some of the rule changes are not surprising, others are very impactful and will markedly change the obligations imposed on covered entities, business associates and subcontractors. Some of the more significant provisions are described in summary below, and a comprehensive review of all the key changes is available at www.poynerspruill.com. Covered entities and business associates will find that a complete project plan is necessary to meet applicable deadlines, and that every day of the remaining six-month compliance window will be necessary to achieve timely compliance.

Important Deadlines

The compliance deadline for virtually every provision of these rules is September 23, 2013. A longer period is provided where updates to existing business associate and data use agreements are required; those agreements may not need to be updated until September 22, 2014 provided they are not modified or renewed prior to that date.

Breach Notification

The current rule requires notice of a security breach if the breach poses a significant risk of harm to affected individuals. In the new rule, OCR eliminates that harm threshold and provides instead that any use or disclosure of protected health information (PHI) that is not permitted by the Privacy Rule will be presumed to be a reportable breach. Covered entities and business associates can defeat this presumption by conducting a risk analysis using factors articulated by HHS, but the agency has made clear its expectation that impermissible uses and disclosures of readily accessible PHI will likely be a reportable breach. This change will mean an increase in the number of breaches reported.

Until the compliance date, the current breach notification rule with its "significant risk of harm" threshold is in effect. To prepare for compliance with the new rule, covered entities and business associates need to do the following:

- Create a risk analysis procedure to facilitate the types of analyses HHS now requires and prepare to apply it in virtually every situation where a use or disclosure of PHI violates the Privacy Rule.
- Revisit security incident response and breach notification procedures and modify them to adjust notification standards and the need to conduct the risk analysis.

continued on p2

HIPAA/HITECH continued from p1

- Revisit contracts with business associates and subcontractors to ensure that they are reporting appropriate incidents (the definition of a "breach" has now changed and may no longer be correct in your contracts, among other things).
- If you have not already, consider strong breach mitigation, cost coverage, and indemnification provisions in those contracts.
- Revisit your data security and breach insurance policies to evaluate coverage, or lack thereof, if applicable.
- Consider strengthening and reissuing training. With every Privacy Rule violation now a potentially reportable breach, it's more important than ever to avoid mistakes by your workforce. And if they happen anyway, during a subsequent compliance review, it will be important to be able to show that your staff was appropriately trained.
- Update your policies The rules require it, and it will improve your compliance posture if HHS does conduct a review following a reported breach.

Business Associates

Much of the Privacy Rule and all of the Security Rule now apply directly to business associates and their subcontractors. Business associate agreements are likely to require updates and, in light of breach requirements and increasing compliance reviews, covered entities should enhance their efforts to review business associate compliance and consider appropriate liability protections in their business associate agreements. It is increasingly common to find covered entities subjecting their business associates to more thorough, pre-engagement assessments, often based on a questionnaire, and both covered entities and business associates can expect business associate contracting to be more strategic and potentially adversarial due to the higher enforcement penalties and compliance risks.

Privacy Requirements

The final rules address multiple privacy issues related to uses and disclosures of PHI, such as communications for marketing or fundraising, exchanging PHI for remuneration, disclosures of PHI to persons involved in a patient's care or payment for care, and disclosures of student immunization records. In addition, individuals have new rights to restrict certain disclosures of PHI to health plans and to request access to electronic PHI (ePHI). Notices of privacy practices, research authorizations, internal policies, and training programs very likely all require updates to address the rule modifications. The modifications also will necessitate revisions to training. Since modifications to training and notices of privacy practices cannot be completed prior to policy modifications, and because implementation and execution of new training and new notices is inherently time consuming, covered entities and business associates are finding value in developing a complete project plan that accommodates interdependent tasks and includes internal deadlines.

p.s.

Business associates and subcontractors are directly liable for their violations, but covered entities also can be penalized for their violations.

Security Requirements

Business associates and subcontractors now must comply with the Security Rule in full. Given the complexities of achieving Security Rule compliance, business associates and subcontractors should begin efforts now to meet the September 23 compliance deadline. Key among these concerns is completion of a comprehensive risk analysis and risk mitigation plan. A multidisciplinary team is often necessary to this process and because many other security decisions will be made based on the results of the analysis, it should be step one in a multi-part security compliance plan.

Genetic Information

To implement the Genetic Information Nondiscrimination Act, HHS has included "genetic information" as a type of health information subject to HIPAA rules, and has imposed restrictions that will prohibit health plans from using genetic information for underwriting purposes. The revisions will affect policies, training and notices of privacy practices and, while a relatively small feature of the new rule, should be included in a compliance project plan.

Enforcement and Penalties

HHS has retained the high penalty structure currently in effect, meaning that penalties can range from $100 to $50,000 per violation depending on culpability, up to an annual maximum cap of $1.5 million on a per provision basis. Business associates and subcontractors are directly liable for their violations, but covered entities also can be penalized for their violations. HHS is now required to conduct compliance reviews if willful negligence is indicated following a preliminary review of the facts.

As with most regulations, the details matter, so we have provided a more comprehensive summary on our website of all the substantive requirements and described in brief how they will impact the regulated community from a practical standpoint. HHS retains discretion to review all other complaints, security breaches and events that suggest noncompliance.

Elizabeth Johnson may be reached at ejohnson@poynerspruill.com or 919.783.2971.

Poyner Spruill LLP
ATTORNEYS AT LAW

NLRB and EEOC May Target Employer Efforts to Keep Employees Quiet During Internal Investigations

By Kevin Ceglowski

Employers frequently instruct employees to not discuss ongoing internal investigations to help preserve the integrity of the investigation. Employers must be aware that the NLRB and the EEOC take the position that such prohibitions could lead to liability under the National Labor Relations Act (NLRA) and Title VII of the Civil Rights Act.

On July 30, 2012, the NLRB held that prohibiting employees from discussing complaints in an internal human resources investigation violated the NLRA because it failed to minimize the impact on employees' rights under the NLRA to engage in protected concerted activity. In the *Banner Health System d/b/a Banner Estrella Medical Center and James A. Navarro* matter, the company's human resources consultant routinely asked employees making a complaint not to discuss the matter with their coworkers while the company's investigation was ongoing. The NLRB ruled this instruction violated the NLRA because the company's concern with protecting the investigation was outweighed by the employees' right to engage in concerted activity. This ruling applies to blanket prohibitions, and the opinion acknowledges that the circumstances of a particular incident may justify a requirement that employees not discuss the investigation.

Following the NLRB ruling, *CCH Employment Law Daily* interviewed Justine Lisser, EEOC Senior Attorney-Advisor and spokesperson, about the EEOC's view of similar prohibitions on employee discussions. Ms. Lisser said, "Broad policies that impose discipline on those who do not abide by strict confidentiality requirements are likely to run afoul of the anti-retaliation provisions of Title VII and/or the other federal EEO statutes [the EEOC] enforce[s]." In particular, such prohibitions will violate the anti-retaliation prohibitions in Title VII. Ms. Lisser did concede that, "An employer who merely suggests that those who are involved in internal investigations of discrimination keep the matters discussed confidential until the investigation is complete out of concern for the integrity of the process is less likely to be found to have violated EEO laws."

p.s.

"Broad policies that impose discipline on those who do not abide by strict confidentiality requirements are likely to run afoul of the anti-retaliation provisions of Title VII..."

Employers who routinely instruct complaining parties and witnesses to not discuss any aspect of internal investigations should keep the *Banner Health Systems* NLRB decision and Ms. Lisser's comments in mind. Employers who have questions about whether the particular circumstances of an investigation justify instructing employees to keep it confidential should consult their employment counsel to analyze whether such an instruction would risk enforcement actions by the NLRB or EEOC. As many employers know, the NLRB is becoming increasingly active in non-union workplaces and the *Banner Health Systems* matter is a warning about yet another area of possible enforcement.

Kevin Ceglowski may be reached at kceglowski@poynerspruill.com or 919.783.2853.

US Citizenship and Immigration Services Publishes New I-9 Form

By Jennifer Parser
jparser@poynerspruill.com
919.783.2955

On March 8, 2013, the U.S. Citizenship and Immigration Services (USCIS) published a new I-9 Form. This Form is completed in part by all newly hired employees no later than the first day of employment. The employee must show the documentation establishing identity and employment authorization no later than the third day after beginning employment, with the designated officer of the employer completing the Form. Employers should make arrangements to use the new I-9 Form since earlier versions are only acceptable until May 7, 2013. After May 7, 2013, all employers must use the revised I-9 Form for each new employee hired in the United States. ■

The Power of "I'm Sorry"

By Ken Burgess

In the 1970s movie *Love Story*, Ali McGraw looks up at her big-screen husband, Ryan O'Neal, and utters the movie's most famous line – "Love means never having to say you're sorry." That line works pretty well in a Hollywood blockbuster, but in the real world, not so much.

The truth is that "I'm sorry" is one of the most powerful phrases in the English language. Think about it. Have you ever faced a friend or loved one who is red-faced and livid with you over some perceived slight, and watched the anger melt away when you sincerely say "I'm sorry?" That's the power of those two words.

In the business world, we also know the power of empathy. A study several years ago examined lawsuits filed by employees against their employers. A shocking number of those plaintiffs identified one primary reason they filed suits – feeling like their employers didn't care, didn't listen, or wouldn't express empathy or sympathy with the employee, regardless of whether the issue involved an employer's wrong doing or just a tough time in an employee's life not caused by his or her employer.

The same thing is true for health care. We all know that health care providers have a legal obligation under state and federal law to keep patients and their families fully informed about all aspects of their care. More importantly, it's just the right thing to do. Many times providers want to express sympathy for health status, failure to thrive or an unintended event. Why not do it more often? It's the fear of being sued and having that "I'm sorry" used against you later in court as an admission of fault.

There's a big difference between expressing sympathy for a patient's or family's situation and admitting the facility or organization caused that situation by negligent care. "I'm sorry for the situation" is not the same as saying "I'm sorry we messed this up," and that's a very important distinction.

Here in North Carolina, health care providers actually have a tool that allows them to say "I'm sorry for your situation" without fear of having that expression of empathy used against them later in court. Thanks largely to the efforts of the North Carolina Health Care Facilities Association, the N.C. General Assembly in 2004 enacted Rule of Evidence 413. This rule dictates what can and can't be introduced in civil court proceedings.

Rule 413 provides "Statements by a health care provider apologizing for an adverse outcome in medical treatment, offers to undertake corrective or remedial treatment or actions, and gratuitous acts to assist affected persons shall not be admissible to prove negligence or culpable conduct by the health care provider in an action brought under Article 1B of Chapter 90 of the General Statutes."

The Rule is designed to encourage, not discourage, expressions of sympathy and offers to help – a public policy goal that many states have embraced. Numerous other states have laws like Rule 413, so providers often can take comfort as they take advantage of this very important tool.

Okay, lawyers are writing this article, so we have to do that lawyerly thing and issue a small word of caution and some practice tips. Obviously, if handled the wrong way – i.e., phrased as "we messed this up and we're sorry" – then Rule 413 and its equivalent in other states may not prevent that statement from being used in a later court proceeding.

Our second caution: Don't let our first caution dissuade you from taking advantage of the freedom to say "I'm sorry and how can we help?" Instead, think about implementing some or all of the practice tips below, perhaps through a documented policy or procedure. These tips are designed to help you work within the protections of rules like Rule 413:

- Think about designating one or two people in your facility or organization to handle the "I'm sorry" discussion. These people should be genuine, represent management and/or the direct care staff with whom the patient and family deal most often, or a combination of the two.
- Think about having two representatives present during these discussions, which serves two purposes – it demonstrates that the expression of sympathy is sincere and comes from the entire staff and, obviously, it provides a witness to ensure that what's said isn't later communicated differently.
- Don't be defensive in these conversations. Instead, be genuine and comforting. Don't assign blame to the patient, family or other staff members, and don't share details of internal quality or peer review discussions or findings related to the matter. The point of these conversations is simply to say "I'm sorry this happened to you and that you're going through this."
- As with everything else we do in health care these days, it's a good idea to document these discussions in the patient's medical record. When doing that, stick to the facts. Document the time and date of the discussion, persons present, what was discussed and plans for follow-up (if made).

Don't let these practical words of wisdom stop you from following your heart and conscience with patients and families. Each provider has to decide how to handle these situations and how best to approach them. Our advice is to follow your conscience, but just use a little common sense along the way. Typically, a sincere "I'm sorry" coupled with a little common sense is great for everybody involved – the patient, the family and your staff. Whether or not those efforts keep disgruntled patients or families from suing you later really isn't the point. Rule 413 and others like it are designed to allow providers to do what they feel is right without having to worry about it later.

Ken Burgess may be reached at kburgess@poynerspruill.com or 919.783.2917.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW