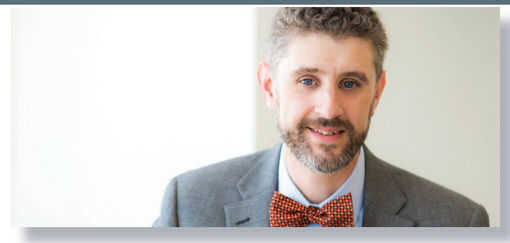
First-Ever OCR Settlement of Enforcement Action against HIPAA Business Associate Due to PHI Breach—$650,000 Monetary Resolution Payment

By Matt Fisher



On June 30, the Office of Civil Rights (OCR) announced the first HIPAA settlement agreement with a business associate. This follows recent settlements with two HIPAA covered entities due, in large part, to the absence of a business associate agreement (BAA) with third-party vendors handling patient protected health information (PHI).

In this first business associate settlement, Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) agreed to settle what OCR determined were potential violations of the HIPAA Security Rule. As with prior settlements with covered entities, this settlement mandates both a two-year corrective action plan and a monetary payment (assessed at $650,000 in this case).

In its role as a business associate, CHCS provided both management and information technology services for six skilled nursing facilities. The breach of the security rule occurred when an unencrypted smartphone was stolen from a CHCS employee. The stolen phone contained a wide variety of PHI for 412 nursing home residents, including Social Security numbers, diagnosis and treatment information, names of family members and guardians, and medication information. As part of its investigation, OCR determined that CHCS had failed to take steps to assess the risks posed by its handling of PHI and had inadequate security protocols in place to minimize the risk of PHI disclosure.

Through this settlement, OCR sent a strong message that HIPAA enforcement is not limited to directly covered entities, but will also be imposed on all business associates that work with those entities. The OCR director stated business associates must conduct "enterprise-wide risk analysis" and maintain a "corresponding risk management plan" in order to comply with the HIPAA Security Rule. It is worth noting that, though this breach actually occurred during the time when CHCS owned the nursing homes, OCR chose to describe this as a settlement with a business associate—perhaps to underscore the importance of business associate compliance.

Under BAA contractual obligations, business associates are specifically required to comply with the provisions of the HIPAA Security Rule and the corollary Breach Notification Rules. Thus, business associates of all types should take advance steps to ensure compliance so they will be prepared in the event of an OCR audit or investigation.

Matthew Fisher's *practice focuses on the representation of health care providers, with an emphasis on HIPAA compliance, privacy and information security matters and Certificate of Need law. He may be reached at 919.783.2924 or mfisher@poynerspruill.com.*

Receive *EndNotes* by Email

If you would like to receive future issues of *EndNotes* and up-to-the-minute news by email, sign up on our website, www.poynerspruill.com.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

SEPTEMBER 2016

ENDNOTES
News for North Carolina's Hospice and Palliative Care Community

Nondiscrimination Final Rule under the ACA Imposes New Requirements on Hospice Agencies

by Iain Stauffer

On May 26, 2016, the United States Department of Health and Human Services (HHS), Office of Civil Rights (OCR), issued the "Nondiscrimination in Health Programs and Activities" final rule, implementing Section 1557 of the Affordable Care Act (ACA). Generally, Section 1557 prohibits discrimination on the basis of race, color, national origin, sex, age, or disability in health programs or activities. The final rule provides guidance to covered entities regarding their legal obligations under Section 1557 and educates consumers about their rights. With certain exceptions, this rule became effective July 18, 2016. Has your agency taken the necessary steps to ensure compliance?

Who is Covered by this Rule?

This rule applies to all entities operating health programs or activities that receive federal financial assistance from HHS, health programs or activities administered by HHS, the Health Insurance marketplaces and the plans offered by issuers that participate in the Marketplaces. The rule refers to these as "covered entities." While federal financial assistance includes Medicaid and Medicare Parts A, C, and D, it does not include payments made under Medicare Part B. Covered entities can include hospitals, health clinics, physicians' practices, community health centers, nursing homes, rehabilitation centers, health insurance issuers, and state Medicaid agencies.

What Does the Final Rule Cover?

Section 1557 builds on existing and long-standing federal civil rights laws and nondiscrimination regulations. This final rule "clarifies and codifies" existing nondiscrimination requirements and provides new protections prohibiting discrimination on the basis of sex in health programs and activities. Generally, an individual shall not, on the basis of race, color, national origin, sex, age, or disability be excluded from participation in, be denied the benefits of, or otherwise be subjected to discrimination under any covered entity.

The final rule sets out requirements in the following areas: meaningful access for individuals with limited English proficiency (LEP); effective communication for individuals with disabilities; accessibility standards for buildings and facilities; accessibility of electronic and information technology; reasonable accommodations; equal program access on the basis of sex; nondiscrimination in health-related insurance and coverage; employer liability for discrimination in employee health benefit programs; and nondiscrimination on the basis of association.

Responsible Employee and Grievance Procedure

If a covered entity has 15 or more employees, the entity must designate a responsible employee to coordinate the entity's efforts to comply with and carry out the responsibilities of Section 1557 and this final rule, which include investigating grievances.

Covered entities with 15 or more employees must also adopt a grievance procedure that incorporates due process standards and provides for a prompt and equitable resolution of grievances. Appendix C of the final rule provides a model grievance procedure covered entities may use. Also, if a covered entity has an existing grievance procedure, the entity may combine it with the grievance procedure required by this rule.

continued on next page

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM
301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

Final Rule under the ACA...

Continued from previous page

Notice Requirements

The final rule imposes new mandatory notice requirements for all covered entities to notify beneficiaries, enrollees, applicants, and the public. Covered entities must comply with the final rule notice requirements by October 16, 2016. The required notice must contain the following:

- That the covered entity does not discriminate on the basis of race, color, national origin, sex, age, or disability in its health programs and activities;
- That the covered entity provides appropriate auxiliary aids and services, including qualified interpreters for individuals with disabilities and information in alternative formats, free of charge and in a timely manner, when such aids and services are necessary to ensure individuals with disabilities have an equal opportunity to participate;
- That the covered entity provides language assistance services, including translated documents and oral interpretation, free of charge and in a timely manner, when such services are necessary to provide meaningful access to individuals with LEP;
- How to obtain the aids and services;
- The identification of and contact information for the designated responsible employee, if applicable;
- The availability of the covered entity's grievance policy and how to file a grievance, if applicable; and
- How to file a discrimination complaint with the HHS OCR.

This notice must be posted in a conspicuous font size in conspicuous physical locations where the covered entity interacts with the public; in a conspicuous location on the covered entity's website, accessible from the home page of the covered entity's website; and in significant publications and communications targeted to beneficiaries, enrollees, applicants, and members of the public. The publications and communications contemplated by the rule would likely include outreach, education, marketing materials, patient handbooks, notices requiring a response, and notices pertaining to rights and benefits. Along with the notice, the covered entity must post taglines in at least the top 15 languages spoken by individuals with LEP in North Carolina. A tagline is a short statement written in non-English languages that indicates the availability of language assistance services free of charge. The HHS website contains a sample and translated versions of a notice of nondiscrimination, statement of nondiscrimination, and taglines for covered entities (http://www.hhs.gov/civil-rights/for-individuals/section-1557/translated-resources/index.html).

Significant publications and communications that are small-size postcards and tri-fold brochures, for example, need only contain an abbreviated nondiscrimination statement and taglines in at least the top two languages spoken by individuals with LEP in North Carolina. Appendix A of the final rule contains samples of the notice and nondiscrimination statement covered entities may use.

Enforcement

The final rule also includes potential enforcement mechanisms. It authorizes lawsuits by aggrieved individuals to challenge alleged violations of Section 1557 and also provides for compensatory damages. In addition, the OCR can enforce Section 1557 through informal means—denying, suspending, or terminating federal financial assistance—or refer the matter to the United States Department of Justice.

What Should a Provider Do?

If covered entities have not already done so, they need to review their policies and procedures to ensure they comply with the nondiscrimination provisions of the final rule. In addition, covered entities with 15 or more employees need to verify they have designated a responsible employee and adopted a grievance procedure. All covered entities need to prepare their notices and taglines to ensure compliance with the posting requirements by the October 16, 2016 deadline. Covered entities should consult with counsel for a detailed review of the nondiscrimination rule, to resolve questions, and to discuss its specific requirements and applicability in order to achieve compliance with Section 1557 and this final rule.

Iain Stauffer's *practice focuses on advising and representing health care providers in Medicare and Medicaid reimbursement, enrollment, compliance, litigation, and regulatory issues. He may be reached at 919.783.2982 or istauffer@poynerspruill.com.*

OSHA's New Rule Impacts the Health Care Industry

by Kevin Ceglowski

The U.S. Occupational Safety and Health Administration (OSHA) recently issued a final rule that becomes effective January 1, 2017, requiring health care industry employers to electronically submit to OSHA injury and illness data from their OSHA logs. This information will then become publicly available on the OSHA website.

As a corollary, and "to ensure the completeness and accuracy of injury and illness data," the final rule also:

- Creates an explicit requirement that employees be informed of their right to report work-related injuries and illnesses free from retaliation;
- Specifically requires that an employer's procedure for reporting work-related injuries and illnesses be reasonable and not deter or discourage employees from reporting; and
- Explicitly prohibits retaliation against employees for reporting work-related injuries or illnesses.

The requirement to report data applies to (1) work locations with 250 or more employees, and (2) work locations with 20 to 249 employees in specific "high-risk industries" identified in the rule which includes several types of health care industries. Specific health care industries that must comply with this rule if they have 20 or more employees at a particular work location are:

- Ambulatory health care services;
- General medical and surgical hospitals;
- Psychiatric and substance abuse hospitals;
- Specialty (except psychiatric and substance abuse) hospitals;
- Nursing care facilities;
- Residential mental retardation, mental health, and substance abuse facilities;
- Community care facilities for the elderly; and
- Other residential care facilities.

Businesses with 250 or more employees at a work location in industries covered by the new record-keeping regulation must submit information from their 2016 Form 300A by July 1, 2017. These employers will also be required to submit information from all 2017 forms (300A, 300, and 301) by July 1, 2018. Starting in 2019, the information must be submitted by March 2 each year. Businesses with 20 to 249 employees in high-risk industries, including the healthcare industries mentioned above, must submit information from their 2016 Form 300A by July 1, 2017, and their 2017 Form 300A by July 1, 2018. Starting in 2019, the information must be submitted by March 2 each year.

OSHA will make the injury and illness data public. After removing any personally identifiable information, OSHA will post the data on its website, and anyone will be able to download it. Employers in the above-referenced high-risk industries (and those with 250 or more employees) should begin planning now to ensure compliance with the January 1, 2017, reporting deadlines.

The new rule also emphasizes that employees who report workplace related injuries and illnesses may not be discriminated against or retaliated against because they have reported such injuries or illnesses. It provides OSHA with the authority to cite an employer for retaliation even in the absence of any employee complaint. The commentary to the rule says:

- Employers must have a reasonable procedure for employees to report work-related injuries and illnesses.
- Employers' reporting procedures cannot deter or discourage reasonable employees from accurately reporting a workplace injury or illness.
- Blanket or automatic post-accident testing policies are prohibited and will be viewed as taking an adverse action against, retaliating against, or discouraging employees from reporting accidents.
- Employers need not specifically suspect drug use before testing, but there should be a reasonable possibility that drug use by a reporting employee was a contributing factor to the reported injury or illness in order for an employer to require testing, and even then, only the employee who caused the accident should be tested rather than everyone involved.

Although the new rule does not prohibit all post-accident/post-injury drug testing policies, OSHA's position is that the circumstances of some accidents make it unlikely drug use was a contributing factor, and therefore testing employees in these situations would be viewed as retaliation. OSHA provides these examples of circumstances where required drug testing would be suspect:

- After an employee reports a bee sting;
- When an employee has a repetitive strain injury;
- After an injury caused by a lack of machine guarding; or
- When a machine or tool malfunctions.

The rule acknowledges many employers implement post-accident/post-injury drug testing policies because they are located in states that offer workers' compensation premium reductions for enacting drug-free workplace policies. Compliance with these workers' compensation programs or other state or federal laws or regulations requiring post-accident/post-injury or reasonable suspicion testing are still permitted.

Employers must also specifically inform employees that (1) they have the right to report work-related injuries and illnesses; and (2) the employer is prohibited from retaliating against employees for reporting work-related injuries or illnesses. Employers also must establish a reporting procedure that does not deter or discourage an employee from reporting work-related injuries and illnesses. These posting and reporting requirements are effective as of November 1, 2016.

In light of OSHA's new rule, employers in the health care industry should review drug testing policies as well as accident/injury reporting policies to ensure they are in compliance.

Kevin Ceglowski, *an employment lawyer in our Raleigh office, may be reached at 919.783.2853 or kceglowski@poynerspruill.com.*