Advisory

JANUARY 2013

If you have any questions about this Advisory, please contact:

MICHELLE WILCOX DEBARGE
860.297.3702
mdebarge@wiggin.com

JODY ERDFARB
203.363.7608
jerdfarb@wiggin.com

Lessons From the Most Recent HHS HIPAA Settlement

On January 2, 2013, the federal Department of Health and Human Services (HHS) announced that Hospice of North Idaho (HONI) agreed to pay $50,000 and entered a two-year corrective action plan to resolve allegations that it violated HIPAA's Security Rule. This settlement reflects the current trend of more vigilant HIPAA enforcement and provides several lessons for HIPAA covered entities and business associates.

THE SETTLEMENT

HHS began investigating HONI after HONI reported to HHS that a laptop containing the electronic protected health information (ePHI) of 441 patients had been stolen in June, 2010. While breaches affecting more than 500 individuals carry more onerous reporting obligations-- requiring notification to the affected individuals, HHS and the media "without unreasonable delay" and in no case later than within 60 days of discovery-- breaches affecting less than 500 individuals do not need to reported to the media, and must be reported to HHS only on an annual basis. Although the stolen laptop contained the ePHI of less than 500 patients, HHS's Office for Civil Rights (OCR) nevertheless launched a broad investigation into HONI's compliance with the Privacy, Security, and Breach Notification Rules.

OCR determined that HONI was not compliant with the Security Rule. Specifically, OCR alleged that HONI did not conduct an accurate and thorough risk analysis of the security of its ePHI until January 17, 2012. OCR also concluded that HONI did not adequately implement reasonable and appropriate security measures for portable devices sufficient to ensure the confidentiality of ePHI until May 1, 2011.

THE LESSONS

Although the fines assessed under the HONI settlement were relatively low compared to fines imposed in other OCR HIPAA settlements, the HONI settlement nevertheless provides several important lessons for covered entities and business associates:

1. Breach Reports May Trigger Investigations. The HONI settlement is the first HIPAA settlement triggered by a report of a breach of ePHI involving fewer than 500 individuals. Covered entities should be aware that breach notification reports are closely reviewed by OCR to determine if further investigation is warranted and should, therefore, be drafted carefully and accurately, and covered entities (and business associates involved in the breach) should be prepared at all times for a potential investigation by OCR.

2. OCR Investigates HIPAA Compliance Broadly. Although OCR's investigation in this case was triggered by a breach report, OCR evaluated HONI's compliance with all of HIPAA's requirements: the Privacy, Security, and Breach Notification Rules. This is consistent with OCR's practice to examine an entity's broader HIPAA practices, even if OCR becomes involved because of a more narrow complaint or concern. Because of this approach, entities should keep HIPAA

CONTINUED ON NEXT PAGE

Lessons From the Most Recent HHS HIPAA Settlement CONTINUED

documentation (including on-going risk analyses, policies and procedures, training logs, and disclosure logs) organized and easily accessible, so that OCR can be provided with evidence of general HIPAA compliance quickly and without difficulty.

3. Safeguards Are Not Enough. OCR concluded that HONI was noncompliant, in part, because it did not complete a Security Rule risk assessment. Many entities mistakenly believe that so long as they have safeguards in place, they are compliant with the Security Rule. This is not true. The Security Rule requires covered entities and business associates to conduct thorough and on-going risk assessments. Regardless of the ePHI in place, OCR wants to see documentation proving that risk assessments have taken place and that the safeguards in place tie back to the assessments.

4. Size Does Not Matter. Although HONI is a relatively small provider, OCR still investigated HONI's compliance, imposed fines and required other corrective actions as part of the settlement. According to the HHS press release announcing the settlement, OCR Director Leon Rodriguez said that the settlement is intended to send, "a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information." While HIPAA's Security Rule allows entities of different sizes to tailor compliance based on its size, OCR will pursue violators of all sizes.

5. OCR is Focusing on Mobile Devices. The violations in this case concerned the failure to assess and implement security mechanisms in regard to mobile devices. As the use of mobile devices, such as laptops and smart phones, becomes more common place in the health care industry, covered entities and business associates need to assess the security mechanisms that they have in place to safeguard ePHI on those devices. OCR has identified mobile devices as a HIPAA risk area. In its press release, HHS announced that a new educational initiative has been launched by OCR and the HHS Office of the National Coordinator for Health Information Technology (ONC) that offers health care providers and organizations practical tips on ways to protect their patients' health information when using mobile devices. More information about this initiative, titled, *"Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information,"* is available at http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.

6. Encryption is Industry Standard. ePHI that is rendered unusable, unreadable, or indecipherable through encryption in accordance with HHS guidance (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html) is exempt from breach notification requirements. If HONI's laptop had been encrypted in compliance with this guidance, HONI would not have been required to report the incident, saving time, money, aggravation, and negative press. With the increased availability of inexpensive and user-friendly encryption methods, encryption is quickly becoming industry standard. As OCR Director Leon Rodriguez said in the HHS press release announcing the settlement, "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."

7. Prior Noncompliance Will Result in Sanctions, Regardless of Current Compliance. Interestingly, the HONI settlement agreement acknowledges that HONI's non-compliance was cured. Security mechanisms to protect ePHI on mobile devices were implemented by May 1, 2011, and security assessments were completed by January 1, 2012. Moreover, according to HONI's press release, before the federal investigation began, upon the report of the theft, HONI immediately began a risk assessment and development of a corrective action plan, including offering credit monitoring to patients who could have been affected. Nevertheless, OCR pursued the imposition of penalties. Covered entities and business associates should know that even if they are fully compliant now, they can still be penalized for any period of time that their compliance was lacking. HIPAA penalties can be assessed per day, although they are generally capped at a certain amount per year. Any entities that are still rolling out HIPAA policies and procedures should ensure that they become compliant as soon as possible to reduce the potential for violations and associated sanctions.