STAY CURRENT
A Client Alert from Paul Hastings

PAUL HASTINGS

January 2013

HIPAA Enforcement Trends: Recent Enforcement Action May be a Sign of Things to Come

BY PAUL A. GOMEZ & JOSH R. HILL

Since the enactment of the Health Insurance Portability and Accountability Act of 1996, as amended, there have been thousands of separate cases of HIPAA violations that have resulted in enforcement by the US Department of Health and Human Services. Adding to the list of enforcement cases, earlier this month HHS announced that it had entered into a settlement for $50,000 with a small hospice provider in Idaho in connection with alleged HIPAA violations. Normally, being one of thousands of individual enforcement actions would not be a significant event, but the facts of this settlement make it noteworthy nonetheless, and may be a sign of future enforcement trends.

Background

In this case, the alleged violation was based on the theft of a single laptop computer containing electronic protected health information of 441 patients. Because the PHI was unencrypted, it was accessible to anyone who had access to the computer, so the theft was considered a breach under HIPAA. The hospice notified HHS of the breach in its annual report, which is required for breaches involving less than 500 individuals (for breaches involving 500 or more individuals, HHS must be notified within 60 days). After investigating the incident, HHS found that the loss of the laptop amounted to a breach of security with respect to the PHI and also that the hospice failed to conduct a risk analysis to safeguard PHI and failed to have policies and procedures in place to cover mobile device security. Specifically, the settlement said that the hospice "did not evaluate the likelihood and impact of potential risks to the confidentiality of [PHI] maintained in and transmitted using portable devices, implement appropriate security measures to address such potential risks, document the chosen security measures and the rationale for adopting those measures, and maintain on an ongoing basis reasonable and appropriate security measures."

Why The Settlement is Significant

The settlement is significant for a few reasons. This is the first reported settlement resulting from a breach involving fewer than 500 individuals. Although historically HHS has focused more attention on much larger breaches, this may be a sign that the federal government is now willing and able to further extend the scope of its enforcement efforts to smaller breaches and smaller entities. Consistent with this, HHS noted that "this action sends 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."

Another noteworthy element of the settlement is the emphasis it placed on risk analysis and the central role that the hospice's failure to conduct a risk analysis played in the settlement. This may signal that HHS is placing a stronger emphasis on the need for providers of all sizes to analyze and identify potential risks before a breach occurs and take proactive protective steps rather than simply reacting after something happens.

Finally, the settlement affirms what HHS and industry commentators have been stating for some time – PHI stored in mobile devices must be protected just like any other PHI, including that stored in desktop computers and other equipment that is not mobile. The fact that the PHI in this case was in a laptop did not reduce the need to protect the information, and, arguably, PHI stored on mobile devices requires even greater protection because of the potential increased likelihood of loss or theft of mobile devices.

Take Away

Perhaps the most prominent message of the settlement is that regardless of the size of a provider or the size of a breach, HHS is willing to investigate and enforce HIPAA. Although this is the first settlement based on a breach involving less than 500 individuals, it likely will not be the last. In addition, the settlement sends a clear message that parties that are subject to HIPAA must perform risk analyses and take steps to protect PHI and minimize identified areas of risk on an ongoing basis, and that the failure to do so can result in enforcement actions. It also offers a reminder to protect mobile devices that carry PHI with at least the same vigilance afforded to other receptacles of PHI. Finally, the settlement further underscores the point that all parties subject to HIPAA should encrypt PHI, not just on in-house computers, but on mobile devices such as laptops as well. If the information is encrypted, then it is far less likely to be considered a breach under HIPAA if the information falls into unauthorized hands.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

Phillip Street
1.404.815.2216
phillipstreet@paulhastings.com

Craig Smith
1.404.815.2366
craigsmith@paulhastings.com

Matt Brohm
1.404.815.2368
mattbrohm@paulhastings.com

Los Angeles

James F. Owens
1.213.683.6191
jamesowens@paulhastings.com

Paul A. Gomez
1.213.683.6132
paulgomez@paulhastings.com

Josh R. Hill
1.213.683.6328
joshuahill@paulhastings.com