INSURANCE/HEALTHCARE

ATTEMPTING TO AVOID THE HIGH COST OF A REPORTED HIPAA BREACH

by Kimberly J. Ruppel and Billee Lightvoet Ward

Preventing unintended or unauthorized disclosure of protected health information is an ever-present goal of all covered entities and business associates. However, protective firewalls and electronic data security measures are not enough to avoid a potentially costly penalty or settlement amount in the event of a breach. In order to defend against assessment of civil money penalties or a negotiated settlement payment, it is important to develop and implement policies, and to train personnel relating to those policies. Such measures are also required to comply with the terms of most cybersecurity insurance policies, or risk a carrier's denial of coverage at a time when it may be needed the most.

In the last 24 months, 349 breaches of unsecured protected health information affecting 500 or more individuals have reported to the Secretary of the Department of Health and Human Services, Office for Civil Rights. Nearly 175 of those breaches occurred in 2017 alone, affecting over 3.2 million individuals in just seven months. From January to July this year, the OCR entered into settlement resolutions related to reported HIPAA breaches for a combined total of approximately $17 million. In 2016, the OCR entered into settlement agreements requiring payment of approximately $48.2 million to resolve reported breaches.

Three of the largest settlement amounts paid this year resulted from failure to develop and implement policies to prevent, report and correct breaches. In February, OCR announced that Memorial Healthcare System paid $5.5 million and agreed to implement a corrective plan to terminate former users' right of access and to review records of system activity. In April, OCR announced that CardioNet paid $2.5 million and agreed to a corrective plan involving risk analysis and risk management procedures designed to address the possibility of theft. In May, OCR announced that Memorial Hermann Health System agreed to pay $2.4 million and adopt a corrective action plan implementing training of its workforce on impermissible use of PHI.

These outcomes demonstrate the importance of being proactive and implementing policies concerning preventing and responding to a breach whether from a malicious external attack or an inadvertent human error from within. Educating and training personnel to recognize whether and how a breach has occurred and how to respond appropriately are important risk management elements of any cybersecurity plan. Executives and employees alike need to be informed about who is authorized to access PHI, what to do if PHI is disclosed, and how to take swift, corrective action, including self-reporting, in the event of a breach.

If a breach occurs, your defense to potential litigation or government penalties will be stronger, and likely the financial impact will be lesser (including the possibility of insurance coverage), with these measures in place. Counsel with the benefit of understanding these steps will help you navigate potential pitfalls. If you have questions about whether your policies are adequate or in need of updating, please contact the authors for assistance.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Insurance/Healthcare law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Kimberly J. Ruppel is a Member in Dickinson Wright's Troy office. She can be reached at 248.433.7291 or kruppel@dickinsonwright.com.

Billee Lightvoet Ward is a Member in Dickinson Wright's Grand Rapids office. She can be reached at 616.336.1008 or bward@dickinsonwright.com.