PUBLICATION

OCR Examines Hybrid Entity Designation in Latest HIPAA Settlement

Authors: Alisa L. Chestler
November 30, 2016

On November 22, 2016, the University of Massachusetts Amherst (UMass) agreed to pay $650,000 and enter into a corrective action plan to settle allegations that it violated the HIPAA Privacy and Security Rules in connection with vulnerabilities that appear to have led to a June 2013 malware attack. The malware attack resulted in the breach of unsecured electronic protected health information (ePHI) of approximately 1,670 individuals. At issue in this settlement, as with others we have seen this year, are allegations focusing on network security vulnerabilities. What is new, however, is OCR's assertion that UMass failed to properly "hybridize" itself and, therefore, implement appropriate protections across all health care components of the University. This is the first OCR settlement that has addressed the "hybrid entity" standard under HIPAA.

According to the OCR press release and resolution agreement in this matter, UMass notified OCR in June 2013 that a workstation at the UMass Center for Language, Speech and Hearing (Center) had become infested with a malware program. The malware infection caused the disclosure of unsecured ePHI, including names, addresses, social security numbers, dates of birth, health insurance information, and diagnosis and procedure codes of approximately 1,670 individuals who presumably had received treatment at the Center.

OCR's investigation, which commenced in August 2013, indicated that while UMass had designated itself a "hybrid entity," it had failed to identify the Center as a health care component subject to the HIPAA rules. As a result, UMass had not implemented policies and procedures at the Center to ensure compliance with HIPAA. OCR further alleged that UMass had not conducted an accurate and thorough risk analysis, nor had it implemented technical security measures at the Center to guard against unauthorized access to ePHI.

The HIPAA "hybrid entity" standard allows organizations, such as universities, to formally designate the health care components of the organization that engage in functions covered by HIPAA and the non-health care components that do not. Health care components must securely segregate PHI from access by or disclosure to non-health care components. Although there are structural, operational and technical requirements for hybrid entity designation, the designation means that only the health care components would be subject to the application of the HIPAA rules and not the organization as a whole. Because the HIPAA rules do not apply to non-health care components, proper identification and designation of all health care components is critical to compliance with the "hybrid entity" standard and with overall compliance with the HIPAA rules. Overlooking covered health care components during the designation process could result in a violation because those missed components would not have policies and procedures in place to adhere to HIPAA's administrative, technical and physical safeguards requirements. That appears to be what happened with UMass and resulted in the corrective action plan and $650,000 monetary settlement. Notably, OCR stated that the amount of the settlement accounted for the fact that UMass operated at a financial loss in 2015, meaning that the amount would likely have been higher under different circumstances.

What this Means for You

The UMass settlement is a clear signal that OCR will be scrutinizing hybrid entity designations in the future. Hybrid designation requires precise documentation and routine updating and review. It also requires implementation of appropriate administrative, technical and physical safeguards to prevent non-health care

components from gaining access to PHI. The interconnection of the hybrid entity organizational standards and the security risk management standards are key takeaways from the UMass settlement.

If your organization has elected to be a hybrid entity under HIPAA, or is considering it, take care to correctly, clearly and completely designate your components. If it has been a while since you designated, take the time to review whether your designations remain accurate. We also suggest that clients create a policy and procedure to review the designation whenever new components are added to an entity – such as a walk-in or community clinic – or when new enterprise-wide systems are implemented.

If you have any questions about hybrid entities, don't hesitate to reach out to Baker Donelson counsel.