Recent HHS Settlement with Phoenix Cardiac Surgery Highlights HIPAA Risks Of Electronic PHI

05.07.2012
05.07.2012

On April 17, 2012, the U.S. Department of Health and Human Service ("HHS") announced that it had entered a Resolution Agreement with Phoenix Cardiac Surgery ("Phoenix") - a four-physician practice based in Arizona - following an investigation of alleged breaches of the HIPAA Privacy and Security Rules. Under the agreement, Phoenix will have to pay $100,000 and comply with a corrective action plan ("CAP"). Although neither the amount of this payment nor the scope of the CAP are particularly noteworthy standing alone, the settlement is significant in that it highlights the care that organizations must take in their handling of electronic protected health information ("ePHI").

HHS's scrutiny of Phoenix focused on its long-standing use of an internet-based email and calendar service in the administration of its practice. The Resolution Agreement indicates that, over the course of a number of years, Phoenix routinely transmitted ePHI to its employees' private email accounts using an internet-based email service and posted ePHI on a publicly accessible, internet-based calendar service. Although use of such technologies by a medical practice is not prohibited under HIPAA, Phoenix did not take any of the steps necessary to protect the privacy and security of the data that it was transmitting through these services. For example, Phoenix failed to identify a security officer, failed to conduct a risk assessment of its use of these services, and failed to obtain business associate agreements to ensure that the service providers were handling ePHI appropriately.

The CAP agreed to by Phoenix addressed the various breaches outlined in the Resolution Agreement largely by requiring the practice to comply with HIPAA. For example, the CAP required Phoenix to adopt HIPAA-compliant policies, train its employees on these policies, and implement appropriate administrative and technical safeguards. Although the CAP does impose certain obligations that exceed the baseline requirements of the Privacy and Security Rules, the plan largely mirrors the basic requirements of HIPAA. Nevertheless, the fact that Phoenix is now subject to the CAP as a result of its use of internet-based services emphasizes the high degree of care that organizations handling ePHI must take to ensure that any use of technology in relation to such ePHI is fully compliant with HIPAA.

Although Phoenix's breach of HIPAA involved specific technologies (i.e., internet-based email and calendar services), the implications of its settlement with HHS extend far beyond the bounds of these technologies. As new methods of electronic communication (i.e., internet-based email, social media, texting, etc.) have become engrained in our daily lives

over the past decade, many health practices and providers have gravitated to these technologies as natural conduits for patient-related communications. However, when such technologies are adopted and used (whether officially or unofficially) by medical practices and their employees, privacy and security implications are often overlooked, ignored, or poorly understood.

As the Phoenix settlement makes clear, HHS is closely scrutinizing the handling of ePHI and playing close attention to the technical details of how practices are managing such data. Therefore, it is incumbent on any practice that is creating, transmitting, communicating, or storing ePHI to ensure that any associated technology is implemented in a way that is fully compliant with HIPAA. Such compliance, particularly the need for business associate agreements, may make the use of certain widely-available and cost-effective technologies (such as internet-based email) impractical in a practice setting, but the action against Phoenix also makes clear that HHS holds small practices, which often have limited resources, to the same standards under HIPAA as larger practices and institutional health care providers.

If you are a covered entity under HIPAA that is creating or managing ePHI, we recommend that you closely review each piece of technology that is involved in your handling or communication of patient data to ensure that proper safeguards are in place.

For more information about this topic, please contact the author or any member of the Williams Mullen eDiscovery and Information Governance Team.

Related People

Related Services

- eDiscovery and Information Governance
- Health Care