WHITE & CASE

Articles

U.S. Department of Health and Human Services Announces First HIPAA Breach Settlement Involving Fewer than 500 Patients

January 2013
White & Case Technology Newsflash
Daren M. Orzechowski, Mariam Subjally

On January 2, 2013, the U.S. Department of Health and Human Services ("HHS") settled its first case involving the unauthorized disclosure of the electronic protected health information ("ePHI") of fewer than 500 individuals. In a resolution agreement signed on December 17, 2012, Hospice of North Idaho ("HONI") agreed to pay HHS $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule.[1]

The HHS Office of Civil Rights began investigating HONI after an unencrypted laptop computer containing ePHI of 441 patients was stolen in June 2010. Through its investigation, HHS discovered that HONI had not conducted a risk analysis of its ePHI, and did not have necessary policies or procedures in place to address mobile device security, all of which is required by the HIPAA Security Rule.[2]

Pursuant to the HIPAA Security Rule, health plans, health care clearinghouses, and healthcare providers who transmit information in electronic form, collectively defined as "Covered Entities" under the law, are required to ensure the confidentiality, integrity and availability of ePHI.[3] Specifically, Covered Entities are required to conduct a thorough analysis of their company to assess potential risks to the confidentiality, integrity and availability of ePHI, and are required to implement policies and procedures to reduce such risks to ePHI.[4]

In this case, HHS found that HONI did not conduct a thorough risk analysis to assess any ongoing risks to the confidentiality of its ePHI. HHS specifically noted that HONI did not assess the risks to ePHI maintained and transmitted using portable devices, such as laptops, and did not adopt or implement sufficient security measures with respect to such portable devices.[5] Pursuant to the resolution agreement, HONI entered into a Corrective Action Plan with HHS. The Corrective Action Plan requires HONI to promptly investigate any allegation that HONI or any of its employees has failed to comply with HONI's privacy and security policies. Additionally, for a period of two years, if HONI determines that a member of its workforce failed to comply with such policies, HONI is required to notify HHS in writing within thirty (30) days.[6]

As stated by Leon Rodriguez, director of the HHS Office of Civil Rights, "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."[7] It is now clear that federal regulators are willing to punish even small data security breaches. Health care providers of all sizes, and the companies who provide services to them, should ensure that they have compliant data security plans in place which are strictly followed by their employees.

HHS recently launched a new initiative to advise Covered Entities on how to best protect patients' ePHI when using mobile devices, such as laptops, tablets and smartphones.[8] More information is available here. Among other suggestions, companies are urged to use passwords or other user authentication measures, install and enable encryption, and research mobile applications before downloading to adequately protect ePHI.[9]

In light of this most recent settlement, companies of all sizes that are considered Covered Entities or who do business with Covered Entities should regularly assess their privacy policies to ensure that they comply with the minimum standards required by HIPAA and HHS, as well as any suggested guidelines issued by the agency. In addition, companies should keep abreast of proposed data privacy regulations and published guidelines to anticipate likely changes in this dynamic area of the law, whether specifically in the healthcare area or more generally as part of the ongoing discussion in the United States about data privacy and protection.

1 - *HHS Announces First HIPAA Breach Settlement Involving Less than 500 Patients*, News Release, January 2, 2013, available here: hhs.gov/news/press/2013pres/01/20130102a.html.
2 - Resolution Agreement, dated December 17, 2012, available here: hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf
3 - 45 C.F.R. §§ 164.302-318.
4 - *Id.* at § 164.308.
5 - Resolution Agreement, dated December 17, 2012, available here: hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf
6 - *Id.*
7 - *HHS Announces First HIPAA Breach Settlement Involving Less than 500 Patients*, News Release, January 2, 2013, available here: hhs.gov/news/press/2013pres/01/20130102a.html.
8 - *Id.*
9 - Your Mobile Device and Health Information Privacy and Security, available here: healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.