

THE NATIONAL LAW REVIEW

\$3 Million Settlement for Two Separate HIPAA Breaches Affecting Over 62,500 Individuals

Thursday, February 14, 2019

Cottage Health and the Office for Civil Rights at the U.S. Department of Health and Human Services (HHS-OCR) recently entered into a [\\$3 million no-fault settlement and three-year corrective action](#) plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA). This was HHS-OCR's last HIPAA related settlement of 2018 – a record year in HIPAA enforcement activity, as detailed in this [DBR on Data blog post](#).

HHS-OCR received notifications from Cottage Health on December 2, 2013, and December 1, 2015, regarding breaches of unsecured electronic protected health information (ePHI) affecting approximately 50,917 individuals and 11,608 individuals, respectively. According to the resolution agreement, the December 2013 breach resulted from a contractor removing the electronic security protections from one of Cottage Health's servers, which made ePHI fully internet accessible and available for download without a username and password. The December 2015 breach arose from an employee activating the wrong website on a database management system server in response to an IT troubleshooting ticket, which also resulted in ePHI becoming fully accessible on the internet.

HHS-OCR alleged that Cottage Health failed to do the following:

- Conduct an accurate and thorough analysis of the potential risks and vulnerabilities to its ePHI as required by HIPAA.
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA.
- Perform a technical evaluation in response to its contractor installing software.
- Obtain satisfactory assurances in the form of a business associate agreement that the contractor would appropriately safeguard ePHI that the contractor maintained on behalf of Cottage Health.

In addition to the significant settlement figure, Cottage Health will undergo a robust corrective action plan, which includes an enterprise-wide risk analysis, implementing a risk management plan, evaluating environmental and operational changes, and developing and distributing policies and procedures that address HIPAA Privacy and Security Rules.

© 2019 Drinker Biddle & Reath LLP. All Rights Reserved

Source URL: <https://www.natlawreview.com/article/3-million-settlement-two-separate-hipaa-breaches-affecting-over-62500-individuals>



Article By

[Sumaya M. Noush](#)

[Drinker Biddle & Reath LLPDBR on Data](#)

[Health Law & Managed Care](#)

[All Federal](#)