Arnall Golden Gregory LLP

Client Alert

Contact Attorney Regarding This Matter:

Neil W. Hoffman
404.873.8594 - direct
neil.hoffman@agg.com

Arnall Golden Gregory LLP
Attorneys at Law

171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031

Two South Biscayne Boulevard
One Biscayne Tower 2690
Miami, FL 33131

1775 Pennsylvania Avenue NW
Suite 1000
Washington DC 20006

www.agg.com

Hospice Provider Becomes Party to First HIPAA Breach Settlement Involving Less Than 500 Affected Individuals

On January 2, 2013, the U.S. Department of Health and Human Services (HHS) announced a settlement agreement with The Hospice of North Idaho (HONI), under which HONI agreed to pay HHS $50,000 and enter into a corrective action plan.[1] This marks the first HHS settlement concerning a breach of unsecured electronic protected health information (ePHI) affecting less than 500 individuals.

As required under 45 C.F.R. Section 164.408,[2] HONI notified the HHS Office for Civil Rights (OCR) following the theft of a laptop containing unencrypted ePHI of 441 individuals. This triggered an OCR investigation of the matter. OCR noted that laptops containing ePHI are regularly used by HONI personnel as part of their field work. OCR also found that since the theft, "HONI has taken extensive additional steps to improve [its] HIPAA Privacy and Security compliance programs." However, over the course of the investigation, OCR also found two things that presumably led to the $50,000 payment and corrective action plan:

- HONI, the hospice provider, had failed to conduct a risk analysis to safeguard the ePHI; and
- HONI had not implemented policies or procedures to address mobile device security.

According to OCR Director Leon Rodriguez, "[t]his 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."[3] [Emphasis supplied.] Mr. Rodriguez also took this opportunity to encourage use of encryption: "[e]ncryption is an easy method for making lost information unusable, unreadable and undecipherable."[4]

There are several take-home messages from this settlement. First, providers who are not HIPAA compliant at the time of a breach of unsecured ePHI

1 *HHS announces first HIPAA breach settlement involving less than 500 patients.* HHS Press Release (Jan. 2, 2013).
2 If a breach affects 500 or more individuals, covered entities must notify the Secretary of HHS without unreasonable delay and not later than 60 days following the breach. If, however, the breach affects less than 500 individuals, the covered entity may notify the Secretary of HHS of such breaches on an annual basis, with such reports being due no later than 60 days following the end of the calendar year in which such breaches have occurred.
3 *Id.*
4 *Id.*

should expect to pay substantial amounts to the government. Second, post-breach corrective actions may not prevent this, though clearly these should be taken (and could favorably affect the amount a provider ultimately has to pay). Third, small providers should not expect a pass. Finally, encryption procedures should be implemented where feasible; this action could ultimately save a lot of time and headache, both for the provider and individuals otherwise affected by a breach, not to mention substantial amounts that that a provider may otherwise have to spend in penalties or settlement.

Click **here**[5] for HHS Press Release.

5 https://www.hhs.gov/news.