SpencerFane®

Providers Need to Take the "Necessary Steps" for HIPAA Compliance

FEBRUARY 26, 2016| PUBLICATIONS

On February 3, 2016, the U.S. Department of Health and Human Services ("Department" or "HHS") issued a statement and released the opinion of the Administrative Law Judge ("ALJ") who found in favor of the Office of Civil Rights ("OCR") determining that a home health agency, Lincare, Inc. ("Lincare") violated the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule requiring Lincare, to pay $239,800 in civil money penalties ("CMP"). The ALJ found clear and convincing evidence that established Lincare violated HIPAA and granted the OCR's motion proposing the CMP. Specifically, the ALJ found that Lincare, which provides various services and equipment to patients in their homes, failed to implement policies and procedures to safeguard records containing patients' protected health information ("PHI"), and it failed to protect against the unauthorized disclosure of its patients' PHI.

The material facts of the case were undisputed and straightforward. Lincare supplies oxygen and other respiratory equipment and services to patients in their homes or alternative sights.[1] Due to the nature of the services, employees are required to take PHI off-site. In this case, the employee maintained such PHI in her vehicle, which was also accessible at all times by her husband. When she eventually moved out of her home, she left the vehicle behind with Lincare's records.[2] Lincare asserted it was not accountable, claiming the records were stolen by the employee's spouse. But, the OCR successfully argued that HIPAA required to take reasonable steps to safeguard PHI, including protecting it from theft and eventually abandonment. The OCR also successfully argued that, even after being informed of the breach of information, the company failed take steps (including revising its policies and procedures) to prevent further disclosures of PHI.[3]

This case represents only the second time in history that the OCR has sought CMP for a HIPAA violation. In the release by HHS, OCR Director Jocelyn Samuels stated "[w]hile the OCR prefers to resolve issues through voluntary compliance, this case shows that we will take the steps necessary, including litigation, to obtain adequate remedies for violations of the HIPAA Rules."[4] She further opined that the decision in the case validated the OCR's investigative findings in that "all covered entities, including home health providers, must ensure that, if their workforce members take protected health information off site, they have adequate policies and procedures that provide for the reasonable and appropriate safeguarding of that PHI, whether in paper or electronic form."[5]

All health care providers can take away some key points from this decision and the comments made by the OCR.

1. **HIPAA Enforcement**. First, the OCR is clearly committed to HIPAA compliance and enforcement. OCR foreshadowed its commitment to enforcement at the end of 2015 following two reports issued by the Office of Inspector General ("OIG"). In those reports, the OIG recommended that the OCR strengthen its oversight of covered entities' compliance with the HIPAA privacy standards. The OCR concurred with the OIG's recommendations and indicated that it was moving forward with a more proactive approach by developing audit programs and the ability to better track breaches affecting fewer than 500 individuals to identify entities with a history of HIPAA compliance issues. The Lincare case supports the OCR's commitment to HIPAA compliance and enforcement. It sends a clear message to all providers that compliance with the HIPAA privacy standards is an expectation; the government will no longer tolerate entities that fail to implement reasonable measures to safeguard protected health information; and the OCR is willing to litigate cases in order to obtain remedies for HIPAA violations.
2. **No Exceptions**. No providers are immune from compliance and liability under HIPAA. For example, Lincare was a home health provider, the breach involved less than 500 individuals, and it was an isolated incident related to a single employee. These are not necessarily the facts of the prototypical headlines related to data breaches we are accustomed to in the news (i.e., the data breaches where millions of individuals' PHI may have been compromised

AUTHORS

- Tina M. Boschert

RELATED INDUSTRIES

- Health Care

BLOG TOPICS

- Health Care Solutions
  - HIPAA

due to a data system hack). Rather, this case was a single issue that highlighted the larger problem of the covered entity — its failure to take reasonable steps to protect its PHI. Again, this decision sends a powerful message to all health care providers (covered entities). The OCR is monitoring all breaches of PHI and will take action against providers that have not implemented appropriate HIPAA policies and procedures, even for isolated incidents related to relatively small breaches of data.

3. **Assess Risk**. Providers need to gauge their own HIPAA compliance and assess their risks and vulnerabilities to protected health information. This includes assessing the organization's (or provider's) compliance with both the HIPAA Privacy Rule and the HIPAA Security Rule. Unfortunately, there is no "one-size-fits-all blueprint" for HIPAA compliance and the level and sophistication of the risk analysis is likely to vary depending on the size, capabilities, and systems of the organization or provider. Generally speaking, in evaluating HIPAA Privacy Rule compliance, health care providers should at least evaluate: the flow of PHI through the organization, the covered entity's policies and procedures, how these policies and procedures align with the requirements of HIPAA, and the entity's current practices regarding patient information. Any gaps in compliance should be identified and addressed. With respect to the HIPAA Security Rule, the OCR, in July 2010, issued guidance that clarifies the expectations with respect to meeting and implementing measures that comply with the HIPAA Security requirements for ePHI. This guidance provides an outline of helpful information for a health care provider to consider when assessing the integrity of an electronic health information system.
4. **Act**. Lastly, health care providers need to be proactive in protecting PHI. This is two-fold. First, covered entities need to have adequate HIPAA policies and procedures in place that provide for the reasonable and appropriate safeguarding of PHI. But simply having policies and procedures in place will not be enough as the Lincare case exemplifies. To ensure HIPAA compliance and ward off OCR enforcement, a provider must take reasonable steps (actions) to: (1) ensure its policies and procedures are adequate and effective in protecting PHI; (2) conduct a risk assessment to identify any gaps and vulnerabilities in its protection of PHI; and (3) in the event of a breach of protected health information, take any additional measures necessary to ensure PHI is secure and not vulnerable to additional disclosure.

The most important lesson providers can take away from the Lincare decision is this: the OCR is willing to take the "necessary steps," to ensure HIPAA compliance, which means health care providers must do the same. All covered entities need to take any and all "necessary steps," to ensure HIPAA compliance and to make certain PHI is adequately protected.

This post was drafted by Tina Boschert, an attorney in the Spencer Fane Overland Park, Kansas, office. For more information, please visit spencerfane.com.

---

[1]Administrative Law Judge Opinion, Director of the Office for Civil Rights, Petitioner, v. Lincare, Inc. d/b/a United Medical, Docket No. C-14-1056, Decision No. CR4505.

[2]*Id*.

[3]*Id*.

[4]Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $239,800, HHS.gov (February 3, 2016) available at http://www.hhs.gov/about/news/2016/02/03/administrative-law-judge-rules-favor-ocr-enforcement-requiring-lincare-inc-pay-penalties.html (last accessed February 26, 2016).

[5]*Id*.

[6]Guidance on Risk Analysis Requirements under the HIPAA Security Rule, Office of Civil Rights, posted July 14, 2010, available at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. (last accessed February 26, 2016).