HALL RENDER
KILLIAN HEATH & LYMAN

HEALTH LAW NEWS

DECEMBER 30, 2013

PHYSICIAN PRACTICE AGREES TO $150,000 HIPAA SETTLEMENT

On December 26, 2013, the Department of Health and Human Services ("HHS") announced that it reached a settlement with a Massachusetts dermatology practice ("Physician Practice") stemming from alleged violations under the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule. The settlement follows an investigation by the HHS Office for Civil Rights ("OCR") upon receiving a report that an unencrypted thumb drive containing the electronic protected health information ("ePHI") of approximately 2,200 individuals was stolen from a staff member's vehicle. This case marks the first settlement with a covered entity for not having policies in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act.

Specifically, the HHS investigation revealed that the Physician Practice had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, the Physician Practice did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

Accordingly, HHS and the Medical Center entered into a Resolution Agreement ("Agreement") in which the Physician Practice agreed to pay $150,000 to HHS and implement corrective measures, which include:

- Designating compliance representatives for each of its facilities;
- Developing, maintaining and revising written policies and procedures that comply with federal privacy standards;
- Establishing administrative, technical and physical safeguards to mitigate security risks and vulnerabilities;
- Distributing approved privacy policies and procedures and training all appropriate staff members on the revised policies and procedures;
- Submitting a written implementation report to HHS to summarize the status of the Agreement's implementation; and
- Filing an annual report with HHS detailing compliance with the Agreement and any findings.

In the press release announcing this action, OCR Director Leon Rodriguez stressed that covered entities of all sizes need to give priority to securing ePHI. Mr. Rodriguez quoted the old saying that "an ounce of prevention is worth a pound of cure," further explaining that a good risk management process involves "identifying and mitigating the risk before a bad thing happens."

PRACTICAL TAKEAWAYS

In light of this development, covered entities of all types should take the necessary steps to ensure that their HIPAA compliance programs are effective, including:

- Developing policies and procedures in all areas required by HIPAA/HITECH;
- Periodically reviewing and revising policies and procedures to ensure that patient information is safeguarded;
- Developing appropriate training for all levels of employees and ensuring that updated policies and procedures are distributed throughout the workforce;
- Ensuring that senior leaders demonstrate a commitment to protecting patient privacy and foster a culture of compliance;
- Establishing physical, technical and administrative safeguards to minimize the risk of inappropriate access to ePHI; and
- Developing and consistently enforcing internal sanctions for workforce members that violate privacy policies and procedures.

More information on this enforcement action, including the Resolution Agreement and the HHS press release, is available here.

If you need additional information about HIPAA and HITECH, please contact Mark J. Swearingen at 317-977-1458 or mswearingen@hallrender.com, Lea H. Lockhart at 317-977-1469 or llockhart@hallrender.com or your regular Hall Render attorney.

Hall Render's HIPAA Impact Series has provided in-depth analysis of HIPAA issues and developments since the passage of HITECH. View our HIPAA Impact Series and sign up to receive updates by visiting www.hallrender.com/impact.