Improper Press Release Leads to $2.4 Million Settlement

May 11 2017

Practice Area: Health Law & Health Information Privacy and Security

This week the U.S. Department for Health and Human Services Office for Civil Rights (OCR) ensconced a settlement for the impermissible disclosure of a patient's protected health information (PHI) without the patient's authorization. The covered entity, a not-for-profit health system located in southeast Texas, must pay $2.4 million and begin implementation of a corrective action plan that involves OCR scrutiny of its HIPAA Privacy Rule compliance.

Impermissible Disclosure

In September 2015, staff at the covered entity's clinic informed authorities that a patient was using a fraudulent identification card. Authorities arrived at the clinic and arrested the individual. While this disclosure of PHI was permissible under the Privacy Rule, the covered entity's disclosure of PHI did not end there. The covered entity then issued a press release regarding the incident. The press release, approved by senior management, included the patient's name in the title of the press release. Senior leaders then further discussed the patient's PHI during subsequent meetings with an advocacy group, state representatives, and a state senator.

Upon discovering media reports related to the press release suggesting that no authorization was obtained to disclose the patient's name to the media and various public officials, OCR began compliance review of the covered entity. OCR found that no authorization was obtained and that the covered entity failed to timely document sanctions imposed against workforce members for the noncompliance.

Settlement

The covered entity and OCR entered into a Resolution Agreement, which includes a two-year corrective action plan requiring the covered entity to:

1. Develop, maintain, revise, and implement written policies and procedures for complying with federal privacy and security standards for PHI, which must include:
    - Instructions and procedures that detail when an authorization to disclose PHI is required;
    - Procedures for disclosure of PHI to law enforcement;
    - Identification of representatives to whom workforce members may contact to inquire about HIPAA compliance;
    - Internal reporting procedures for HIPAA violations; and
    - Application and documentation procedures for sanctions against workforce members for failure to comply with HIPAA or these policies and procedures.
2. Distribute the policies and procedures implemented above to all workforce members, and require the workforce members to agree to comply with the policies and procedures;
3. Assess and update the policies and procedures annually;
4. Notify OCR of any workforce member's failure to comply with the covered entity's policies and procedures (not just procedures related to Privacy Rule compliance);
5. Implement Privacy Rule training for workforce members specifically tailored to each workforce member's function with the covered entity; and
6. Submit annual reports detailing the covered entity's corrective actions taken during the year.

OCR clearly places a great deal of emphasis on the implementation of properly updated policies and procedures regarding the disclosure of PHI and the successful education and enforcement of these policies and procedures for workforce members. This settlement reinforces the importance for covered entities to ensure that its workforce members are properly trained to comply with the Privacy Rule, and that covered entities properly enforce policies and procedures and sanction workforce members who fail to comply with the Privacy Rule or the covered entities' policies and procedures. The former helps to prevent impermissible disclosures such as the one at issue here, and the latter shows that the covered entity is serious about and committed to complying with HIPAA.
