

\$25K OCR HIPAA Settlement for Physical Therapy Provider

A physical therapy provider agreed to an OCR HIPAA settlement following allegations that it had exposed patient PHI.

February 22, 2016 -- The U.S. Department of Health and Human Services Office for Civil Rights (OCR) agreed to a HIPAA settlement with Complete P.T., Pool & Land Physical Therapy, Inc. (CPT) after alleged violations that the physical therapy provider potentially exposed patient information.

CPT must pay \$25,000 as well as implement a corrective action plan, according to OCR, and must report on its compliance efforts for one year.

All covered entities - even physical therapy providers - need to have adequate policies and procedures to obtain an individual's authorization for marketing purposes. This includes when posting information on a website or social media pages.

OCR explained in a statement that it received a complaint on August 8, 2012 that CPT had impermissibly disclosed patient PHI. The information was allegedly exposed when the provider "posted patient testimonials, including full names and full face photographic images, to its website without obtaining valid, HIPAA-compliant authorizations."

"The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes," OCR Director Jocelyn Samuels said in a statement. "With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing."

Samuels added that all covered entities - even physical therapy providers - need to "have adequate policies and procedures to obtain an individual's authorization for such purposes." This includes when posting information on a website or other social media pages.

The OCR investigation into CPT found the following violations:

- Complete P.T. failed to reasonably safeguard PHI;
- The provider impermissibly disclosed PHI without an authorization; and
- Complete P.T. failed to implement policies and procedures with respect to PHI that were designed to comply with HIPAA requirements regarding authorization.

[According to the resolution agreement](#), CPT also needs to properly train its workforce in how the HIPAA Privacy Rule applies to the provider.

“At a minimum, training shall cover all of the topics that are necessary and appropriate for each member of the workforce to carry out that workforce member’s function within CPT, with respect to the use and disclosure of PHI,” the agreement reads.

Moreover, the employee training needs to be reviewed annually and updated as necessary to “reflect changes in Federal law or HHS guidance.” Should any audits, reviews, or other developments show a need for change, the training will also need to be adjusted.

“If CPT determines, after review and investigation, that a member of its workforce has failed to comply with its Policies and Procedures or that there has otherwise been a violation of the HIPAA Rules, CPT shall notify HHS in writing within thirty (30) days,” according to OCR. “Such violations shall be known as ‘Reportable Events.’”

As previously discussed on HealthITSecurity.com, HHS requires organizations to be specific with their disclosure authorization policies and procedures. For example, an authorization needs to be written in specific terms and all authorizations must be in “plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.”

A key aspect to the HIPAA Privacy Rule is the “minimum necessary,” which states that covered entities “must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

Complete article posted here: <http://healthitsecurity.com/news/25k-ocr-hipaa-settlement-for-physical-therapy-provider>

NEED HELP WITH HIPAA COMPLIANCE?

Order our complimentary HIPAA Pocket Guide by sending an email to
Info@JDLHealthTech.com

Or, complete the order form at this link:

<http://www.jdlhealthtech.com/services/hipaa-pocket-guide>