Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Beware Of Posting Patient Testimonials On Your Website

Plus: Get ready for new regs governing substance abuse confidentiality.

Watch out: The **HHS Office for Civil Rights** (OCR) is enforcing the HIPAA Privacy Rule requirements for obtaining valid authorization before using protected health information (PHI) for marketing purposes.

Case in point: On Feb. 16, OCR announced a resolution agreement with Los Angeles-based **Complete P.T., Pool & Land Physical Therapy** (Complete P.T.) for alleged HIPAA violations stemming from patient photographs the provider posted on its website without authorization.

In August 2012, OCR received a complaint alleging that Complete P.T. posted patient testimonials, including full names and full-face photographic images, on its website without first obtaining HIPAA-compliant authorizations to do so. OCR's subsequent investigation revealed that Complete P.T. failed to reasonably safeguard PHI, impermissibly disclosed PHI without authorization, and failed to implement appropriate policies and procedures regarding the use of PHI and obtaining HIPAA-required authorizations.

Pay attention: This particular case highlights the HIPAA Privacy Rule's protections for individuals concerning the use of their PHI for marketing purposes. With limited exceptions, the Privacy Rule requires that you obtain an individual's written authorization before using or disclosing PHI for marketing purposes.

"All covered entities, including physical therapy providers, must ensure that they have adequate policies and procedures to obtain an individual's authorization for such purposes, including for posting on a website and/or social media pages, and a valid authorization form," OCR Director **Jocelyn Samuels** said in the Feb. 16 announcement.

Under the resolution agreement, Complete P.T. must pay $25,000, adopt and implement a corrective action plan (CAP), and provide annual reporting of its compliance efforts for one year. The settlement agreement is effectively an admission of civil liability by Complete P.T.

To read the resolution agreement and CAP, go to http://www.hhs.gov/sites/default/files/cpt-res-agreement.pdf.

You'll Soon See Updated Regs For Substance Abuse Records

Nearly 30 years have passed since the **U.S. Department of Health & Human Services** (HHS) has made any significant changes to the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records. But that's all about to change.

The HHS Substance Abuse and Mental Health Services Administration (SAMHSA) recently proposed amendments to the substance abuse confidentiality regulations, citing important changes to the U.S. healthcare system, and the subsequent need to update and modernize the regulations. HHS published the proposed rule, "Confidentiality of Substance Use Disorder Patient Records," in the Feb. 9 Federal Register.

According to SAMHSA, the regulations need updating to recognize "new models of integrated care that are built on a foundation of information sharing to support coordination of patient care, the development of an electronic infrastructure

for managing and exchanging patient information, and a new focus on performance measurement within the healthcare system."

"The last substantive changes to the regulations date back to 1987," noted partner attorney **Laurie Cohen** in a Feb. 11 **Nixon Peabody LLP** blog posting. In the proposed rule, SAMHSA intends to:

1. Amend key regulatory definitions, including "program" as it applies to "general medical facilities" and "general medical practices;"
2. Change patient consent requirements for disclosing patient records, including the use of a generalized designation for authorized recipients in certain circumstances;
3. Allow electronic signatures when consistent with applicable state law;
4. Change the patient notification requirement to allow electronic notices; and
5. Clarify the services that Qualified Service Organizations may provide to include population health-management services.

You can submit comments on the proposed rule to SAMHSA until April 11. The proposed rule is available at www.federalregister.gov/articles/2016/02/09/2016-01841/confidentiality-of-substance-use-disorder-patient-records.

Your Paper Records Still Present A Serious Security Weak Spot

Despite all the focus on cyber security and hacking incidents, the reported large breaches this February have reinforced the concern that paper records can cause just as much trouble in your HIPAA compliance as your electronic systems and devices.

In February, there were 17 total breaches affecting 500 or more individuals, according to the **HHS Office for Civil Rights** (OCR) "Wall of Shame." As usual, healthcare providers accounted for the vast majority of the reported breaches, with 11 incidences, followed by three breaches from health plans and another three from business associates.

Most (eight) reported breaches involved unauthorized access/disclosure, while theft accounted for five breaches. Two breaches stemmed from hacking/IT incidents and another two were due to loss.

For the reported "location of breached information," the breaches in February were a mixed bag. Five breaches involved paper/films, three involved network servers, and two involved laptops. Other locations included email (two breaches), electronic medical record (one), desktop computer (one), and "other" (three).

By far, the largest breach occurred at healthcare provider **Radiology Regional Center** in Florida, affecting 483,063 individuals. The breach occurred due to loss of paper/films. You can view the OCR's "Wall of Shame" at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Yes, You Should Send Patient Records To These 3rd Parties

If you need more clarification on how much you can charge for providing patients with copies of their health records, you now have some new materials from the federal government.

In a new fact sheet containing a set of FAQs, the **HHS Office for Civil Rights** (OCR) clarified the fees you may charge individuals for copies of their health information and individuals' right to have their health information sent directly to a third party.

You may charge individuals only a reasonable, cost-based fee for the labor and supplies associated with making the copy, whether on paper or in electronic form, of their health records, according to OCR. Also, individuals have the right to request that you send their health information directly to a third party for example, to a friend or family member, another healthcare provider, researchers, or even a personal health record, mobile health app or other consumer tool.

Link: To access the new fact sheet, go to www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

Utilize A Crosswalk To Shore Up Your Security Efforts

Weeding through the mandatory regulations, industry best practices and myriad of other cybersecurity frameworks can be confusing. Here's a new crosswalk tool that can help you to make better-informed decisions on how to frame your own cybersecurity strategy.

On Feb. 24, the **HHS Office for Civil Rights** (OCR) released a crosswalk that identifies "mappings" between the HIPAA Security Rule and the **National Institute of Standards and Technology** (NIST) Framework for Improving Critical Infrastructure Cybersecurity. Unlike the HIPAA Security Rule, the NIST Cybersecurity Framework is not mandatory for healthcare organizations. The crosswalk also includes mappings to other commonly used security frameworks containing best practices for bolstering your protection of electronic data.

Significance: "The sensitive information maintained by healthcare providers and health plans has become an increasingly attractive target for cyberattacks," HHS warned. "The need for healthcare organizations to up their game on health data security has never been greater."

And although covered entities (CEs) and business associates (BAs) are reporting to OCR that they're working hard to adequately protect their PHI, "we also know from our HIPAA enforcement work that far too frequently entities are leaving PHI vulnerable to breach and access by unauthorized persons," HHS noted.

HHS also believes that the new crosswalk will help healthcare organizations that have already aligned their security programs with either the NIST Cybersecurity Framework or the HIPAA Security Rule to identify possible gaps in their programs. You can view the new crosswalk at www.hhs.gov/sites/default/files/NIST CSF to HIPAA Security Rule Crosswalk 02-22-2016 Final.pdf.