Health Information Compliance Alert

Enforcement News: Help Patients Access Their PHI with a New Form From AHIMA

Plus: Technology overload can impact healthcare in a negative way.

Patients with access to their protected health information (PHI) are more invested in their care and more willing to abide by doctors' orders. However, despite the best intentions, it can be challenging for patients to request and gain that important information.

The American Health Information Management Association (AHIMA) created a new form for providers to "streamline the process when patients request their PHI under HIPAA and comply with the timeframe and fees set out by the Office for Civil Rights' (OCR) guidance of 2016," says AHIMA's "Advocacy and Policy Efforts" section on its website.

The AHIMA form is free, and it's easy to read, download, and use. It offers detailed reasoning with HHS and OCR links that explain why you must follow certain HIPAA protocols (i.e. 30-day timeframe for delivery of PHI to patient) when patients request their medical records. The form can be "customized by providers and organizations to capture the data you need as well as organizational contact information," the AHIMA guidance notes.

Resource: For a link to the AHIMA information and patient request form, visit http://www.ahima.org/about/advocacy/efforts.

In other news ...

Cyber criminals continue to make their mark with ransomware attacks, taking down healthcare systems on a daily basis and exposing patients', providers', and hospitals' privacy and security. And with HIPAA compliance repeatedly compromised as thousands of individuals' ePHI is lost or manipulated, patients' care and treatment (as well as practices' livelihoods) are at risk.

In the July issue of the OCR's Cybersecurity Newsletter, the federal organization focuses on the increase of ransomware attacks and how the rise in mobile hardware and health IT might be to blame.

"The healthcare sector's risk landscape continues to grow with the increasing number of interconnected, 'smart' devices of all types, the increased use of interconnected medical record and billing systems, and the increased use of applications and cloud computing," notes the July Cybersecurity Newsletter. The release also addresses the perennial question of who should be trained on HIPAA protocols and how often, particularly with the avalanche of breaches caused by malware and social engineers pummeling the nation's healthcare industry.

Reminder: The newsletter guidance advises covered entities and their associates to remember the HIPAA Security Rule and its requirements that necessitate implemented training programs with updates for all staff members. "Note the emphasis on all members of the workforce, because all workforce members can either be guardians of the entity's PHI or can, knowingly or unknowingly, be the cause of HIPAA violations or data breaches," indicates the OCR.

The Cybersecurity Newsletter also offers insight into how often training should take place and how you should document it. Consider these questions as you organize your HIPAA compliance training:

- Are you analyzing your risks and using that data to plan the timeliness of your practice HIPAA education? Do you need to revisit your assessments and checklists weekly, monthly, or annually?
- Does your practice IT manager or third-party vendor update you and your staff on the most recent threats and how to combat them?

- What resources do you utilize now in your training? Do you need to upgrade and increase the materials to better manage your cybersecurity?
- Are you documenting the assessments, analysis, management, and training?

Tip: If you are audited after a breach, the first thing the OCR will ask is for written details of your HIPAA plan and staff training. Prepare now to avoid problems after a breach happens.

Resource: To read the July 2017 issue of the OCR's Cybersecurity Newsletter, visit https://www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf.