Health Information Compliance Alert

Enforcement News: ONC Wants Your Opinion on Improving EHRs

Plus: Malware incident impacts over 500,000 patients.

Though the recent statistics suggest most physicians and hospitals are on board the EHR-implementation train, problems still remain that impede practice workflows.

The HHS Office of the National Coordinator for Health Information Technology (ONC) is offering a way for interested stakeholders to be part of the federal changes to Certified EHR Technology (CEHRT). The initiative, titled "ONC's Easy EHR Issue Reporting Challenge," hopes to "help EHR users identify, document, and report a potential health IT safety issue when it happens," says **Andrew Gettinger, MD**, ONC Chief Medical Officer in a blog post.

The end-goal is to inform and improve, making EHRs more efficient and easier to use. The submission deadline is Oct. 15, 2018.

To read Dr. Gettinger's blog post with links to sign up for the challenge, visit www.healthit.gov/buzz-blog/electronic-health-and-medical-records/a-new-challenge-competition-can-you-help-make-ehr-safety-reporting-easy/.

In other news...

A Baltimore-based healthcare provider disclosed a major malware attack and subsequent HIPAA breach that it had uncovered from 2016. The HHS Office for Civil Rights (OCR) wall of shame highlighted the Maryland organization's results: the exposure of the protected health information (PHI) of 538,127 individuals.

"On March 18, 2018, we discovered that malware infected the servers that hosts LifeBridge Potomac Professionals electronic medical record, and LifeBridge Health's patient registration and billing systems," stated a LifeBridge press release on May 16, 2018. "We immediately began an investigation and engaged a national forensic firm. Our investigation determined that an unauthorized person accessed the server throughLifeBridge Potomac Professionals on September27, 2016."

The healthcare organization added, "The information potentially accessed may have included patients' names, addresses, dates of birth, diagnoses, medications, clinical and treatment information, insurance information, and in some instances, social security numbers."

Currently, LifeBridge Health maintains that no nefarious circumstances or activity has resulted yet from the cyber attack and stolen PHI.

Read the release at www.lifebridgehealth.org/Main/SecurityIncident.aspx.