Readiness for Audits Essential for IG Programs

Save to myBoK

By Angela Rose, MHA, RHIA, CHPS, FAHIMA

AHIMA hosted a very engaging Twitter chat on Thursday, April 14, 2016, about the role that privacy and security plays towards launching and implementing successful information governance (IG) programs. To see Tweets from the chat and other information governance (IG) related Tweets, view the #IGNow hashtag on twitter.com. The chat included answers to some challenging questions as well as information on the various resources available in the industry to get your IG program off the ground and running.

A strong IG program will have privacy and security embedded at its core. Privacy and security is also an integral part in helping an organization not only protect its health information, but also keep it stable and ready should the organization be audited. The HITECH Rule mandated periodic audits of covered entities and business associates on the status of their privacy and security compliance. The purpose of the audits is to provide the Office for Civil Rights (OCR) with a pulse on the overall compliance with HIPAA as a nation—to identify weaknesses, gaps, and areas where organizations need help and guidance.

On March 21, 2016, Deven McGraw, deputy director for health information privacy at OCR announced that the HIPAA Phase 2 audits officially started. The HIPAA Phase 1 audits were completed in 2012 of 115 covered entities. The Phase 2 audits are expected to be completed by the end of 2016 to include 200-250 covered entities and business associates.

OCR will first send notification (via e-mail) to selected covered entities and business associates asking for contact information confirmation. The entities will then have 10 days to respond to that request. If an entity does not respond, they can still be added to the pool of potential auditee candidates. OCR will select auditees from that pool and send a formal letter (via e-mail) confirming the impending audit.

This round of audits will include desk audits and onsite audits. It was stated that a desk audit does not necessarily mean the entity will have an onsite audit. OCR will identify entities for onsite audits as they deem are necessary. An onsite audit is estimated to last three to five days. Whether the audit is a desk audit or an onsite one, a report will be issued to the audited entity one the audit is completed. The entity will have 10 days to respond and comment. A final report will be issued 30 days from any comments submissions.

Readiness for audits conducted by external entities in order to demonstrate compliance is an essential function of an organization's IG program. Information governance is a proactive strategy, the byproduct of which is keeping covered entities and business associates prepared for such an audit. Privacy and security only comprises one component to an effective and successful IG program. It should be the root and core base of your program acting as the glue to nurture and grow the rest of the program.

Angela Rose (angela.rose@ahima.org) is a director of HIM practice excellence at AHIMA.

Original source:
Rose, Angela Dinh. "Readiness for Audits Essential for IG Programs" (Journal of AHIMA website), April 28, 2016.