COSMOS
Navigate the Compliance Universe

Compliance Today - August 2021
Patient access and the path to compliance

By Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB

Rita Bowen (rbowen@mrocorp.org) is VP of Privacy, Compliance, and HIM Policy, MRO, Norristown, PA.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule generally requires HIPAA covered entities—health plans and most healthcare providers—to provide individuals, upon request, with access to protected health information (PHI) about them in one or more "designated record sets" maintained by or for the covered entity.[1] This includes the right to inspect and/or obtain a copy and the right to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. This right applies as long as the covered entity, or its business associate, maintains the information, regardless of the date the information was created, and whether the information is maintained in paper or electronic systems on-site, remotely, or is archived.

Providing patients access to their PHI is a top priority. Patients need secure, timely access to their medical information to make informed decisions and manage their own care. The ever-increasing enforcement actions by the Office for Civil Rights (OCR) at the U.S. Department of Health & Human Services are intended to empower patients and hold healthcare providers accountable for failure to meet HIPAA requirements. This article provides valuable insights and guidance to help organizations prepare for full compliance.

OCR focus on patient right of access

The OCR's *HIPAA Audits Industry Report*[2] released in late December 2020 stated that 89% of audited covered entities failed to show they were correctly implementing the individual right of access. The report noted many compliance gaps, including insufficient policies and procedures for providing access. For example, the OCR found that some policies incorrectly stated that the covered entity could deny access to PHI, and other policies lacked guidance around providing requests for information to a designated third party.

Overall, these covered entities are largely operating on their own and do not have access to a security or compliance officer who has the knowledge and experience needed to understand and create policies to ensure compliance. Because release of information (ROI) is such a detailed and intricate process, all covered entities must ensure compliance with the standards. One way to achieve that goal is to have a specific department dedicated to the effort under the guidance of professionals with expertise to properly implement and enforce policies and procedures. It is essential to designate staff who are specifically responsible to learn the guidelines, implement policies and procedures required to follow the guidelines, ultimately enforce the guidelines, and continually assess and adjust as needed.