COSMOS
Navigate the Compliance Universe

Compliance Today - May 2020
'Low-hanging fruit' and other recent HIPAA compliance items

By Rachel V. Rose, JD, MBA; and Patrick Ouellette, Esq., CIPP/US

Rachel V. Rose (rvrose@rvrose.com) is Attorney at Law, PLLC, in Houston, Texas. **Patrick Ouellette** (pouellette583@gmail.com) is Assistant General Counsel at the Massachusetts Executive Office of Health and Human Services.

Recently, Roger Severino, director of the Department of Health & Human Services (HHS) Office for Civil Rights (OCR), indicated that in relation to the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[1] "[f]or enforcement purposes, there's still a lot of low-hanging fruit."[2] The 2019 year-end trend of OCR issuing fines for violations of the Privacy Rule,[3] the Security Rule,[4] as well as the intersection of various state biometric and privacy laws,[5] highlights the value of compliance and how it ultimately reduces the risk of a potential OCR enforcement action.

From September through December 2019, OCR issued several financial penalties related to Privacy Rule[6] violations. Importantly, two cases (Bayfront Health St. Petersburg[7] and Korunda Medical LLC cases[8]) related to failures to provide patients access to their own medical records within the time frame and fee structure prescribed by HIPAA, resulting in the first enforcement actions and settlements under OCR's Right of Access Initiative. The Privacy Rule also rears its head in times of natural disasters, infectious disease outbreaks, and other emergencies. For example, the COVID-19 outbreak serves as a reminder to providers as to what can and cannot be disclosed, as well as whom it may be disclosed to.

Analysis

The purpose of this article is to hone in on what is considered "low-hanging fruit" by OCR; review the February 2020 bulletin: *HIPAA Privacy and the Novel Coronavirus*[9] in light of current events; and provide compliance best practice areas that can mitigate the risk of an actionable HIPAA violation or breach of protected health information (PHI).

Low-hanging fruit

The Security Rule[10] and Privacy Rule[11] make it very clear that certain technical, administrative, and physical safeguards need to be implemented in order for an organization to be considered compliant with HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[12] Neither HIPAA nor the HITECH Act are new, with HIPAA stemming back to 1996, and the HITECH dating back to 2009. Therefore, it's perplexing that "[t]here are a lot of entities that are not doing the basic steps to make sure that they have proper, for example, cybersecurity protections in place. They're not doing the comprehensive risk analyses on the front end."[13] No entity is exempt from this particular requirement, as illustrated by the $1.6 million penalty imposed by OCR in November 2019 on the Texas Health and Human Services.[14]

According to HHS's website, "The HIPAA Security Rule establishes national standards to protect individuals'

electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[15]

Examples of technical, administrative, and physical safeguards, all of which should be addressed in an annual comprehensive risk analysis, include: access controls (i.e., unique user ID and password, access logs); adequate encryption (minimum 256 bit) both at rest and in transit; adequate annual training; and comprehensive policies and procedures. Likewise, as indicated on the HHS website,

> "The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections."[16]

As previously mentioned, the privacy of one's PHI, as well as the right to examine and obtain a copy of PHI, is inherent in HIPAA, and the failure of covered entities to provide access was a focus of OCR in the latter part of 2019. Thus, during an annual risk analyses, the Privacy Rule should be given equal attention to the Security Rule.[17]