COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 3. March 11, 2021
Points to Consider When Beefing Up Procedures for Access Requests

By Jane Anderson

HIPAA privacy experts recommend a series of steps for health care entities to take to beef up their medical records access programs—and potentially steer clear of HHS Office for Civil Rights (OCR) penalties in the process.

- **Make access a priority.** "As the recent sixteenth HIPAA noncompliance settlement for not complying with the right to access requirement demonstrates, organizations must take this activity much more seriously, put aside some time to think through the actions necessary to fulfill such requests, and create procedures for their organization to follow as soon as they receive such requests," said Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor.

  "The number one situation I've seen over the years is that CEs [covered entities] don't prepare procedures for responding to a right of access," Herold explained. "They underestimate the activities necessary to respond to such requests and simply assign the responsibility to an individual, team or role, and then it stops there after making that assignment. Those individuals/teams/roles then do nothing. Most think, 'Sure; if a request comes in, I'll pull the file and send them a copy.' Then when the requests start coming in, they realize that, 'Oops, we should have thought this through better.' They soon find that they don't know where all the requested information is located throughout the organization, within their business associates and/or that the information was not retained, so then they cannot provide the information going back six years as required, or they simply do not know where the information is located and don't know where to start looking."

  This dynamic takes the situation from bad to worse, Herold said. "They will then often simply not respond to the request, with the expectation that the individual asking for the information will simply forget about it," but then that violates more of the HIPAA requirement by ignoring the requestor.

  The bottom line: determine in advance how to fulfill requests and put the procedures in place to do so.

- **Designate a privacy officer who is responsible for implementing these procedures.** This position is key to the right of access, said attorney Samantha Gross, associate with Saul Ewing Arnstein & Lehr LLP in Philadelphia. "The privacy officer should ensure compliance with the policies and procedures, including those related to the right of access. This means updating the policies as necessary and training workforce members and relevant business associates on those policies and procedures," Gross said. "The privacy officer or another designated individual should also review the provider's business associate agreements to ensure business associate agreements are in place and business associates are in compliance with the entity's policies and procedures. Several recent OCR settlements involved business associates."

- **Emphasize staff training on privacy and access.** "Many health care organizations, particularly smaller physician practices, worked with a HIPAA consultant or purchased an off-the-shelf manual of HIPAA policies and procedures many years ago, put the manual on the bookshelf, and since that time have been under the impression that they were in compliance with HIPAA," said attorney Eric Fader, a partner with Rivkin Radler in New York City. "This is obviously not good enough," he said. According to Fader, the two

most commonly overlooked requirements in HIPAA are (1) conducting periodic security risk assessments (not relevant to access but most important nonetheless) and (2) properly training and retraining the workforce no less than once per year. "OCR has been auditing providers for many years," and the Centers for Medicare & Medicaid Services and OCR have been focusing on patients' right of access since 2019, Fader said.

- **Identify and document all locations where health information is located.** This can pay security benefits, along with helping the organization comply with access requirements, Herold said. "When they do this, they will almost always discover health data stored in locations that they had not known about, and will discover old health data that they should have disposed of decades ago, along with discovering security problems for where the information (in all forms and on all types of media) is stored," she explained, and "not only are they complying with the HIPAA privacy rule right of access requirements, they are also fulfilling security rule risk management requirements to identify risks. And then they continue to comply with more security rule requirements by implementing safeguards appropriate for their own organization to safeguard those newly discovered storage areas—resulting in better security and reduced risk for privacy breaches."

- **Make sure you're responding in a timely fashion.** Timing is key, Gross explained. "Many of the settlements demonstrate that health care providers are failing to comply with the timing required—specifically that covered entities must respond to a right of access request no later than 30 days after receipt," according to 45 C.F.R. § 164.524(2), Gross explained. "Covered entities must also provide access to protected health information in the form and format requested by the individual. Many of the settlements involved lengthy…response times after the initial request for records. If a provider is unable to respond or is uncertain about how to respond to a request, the provider should seek assistance *immediately* given the 30-day window in which it must respond."