Report on Patient Privacy Volume 21, Number 5. May 06, 2021 OCR Investigator: Goal Is to Uncover 'Root Cause,' Remedy Harm From Violations

By Theresa Defino

Given the hundreds of thousands of HIPAA covered entities (CEs) and business associates (BAs) and the two dozen or so enforcement actions the HHS Office for Civil Rights takes annually, the odds are exceedingly slim that an organization will find itself in a formal sanctions process with OCR.

On the other hand, OCR does investigate every breach affecting more than 500 individuals as well as other complaints that come in, particularly egregious situations, and if things don't go well, an organization could find itself dogged by the agency's investigators.

So, wouldn't it be nice to get inside the mind of an OCR investigator? Enter John Haskell, an investigator in OCR's Mid-Atlantic Region, who joined the agency approximately 18 months ago. Since that time he has handled "close to 400 complaints," gaining experience with a range of privacy issues and organizations, both "large and small."

Among the insights Haskell has gleaned: OCR *really* doesn't like when it receives repeat complaints, and it is *especially unhappy* when a CE or BA is unresponsive to its entreaties. He also gave some tips on how to draft a successful response to an OCR data inquiry and when it might be okay to give him a phone call.

Haskell, whose jurisdiction involves Pennsylvania, Virginia, West Virginia, the District of Columbia, Maryland and Delaware, chatted with Scott Intner, chief compliance officer for GW Medical Faculty Associates, at a recent conference[1] sponsored by the Health Care Compliance Association, which publishes *RPP*. Intner said he had "worked through a couple of incidents together" with Haskell and wanted others to understand an investigator's perspective and world view.

Haskell said his case load averages "in the mid-80s," with about 25% comprising right-of-access complaints, a volume he expects will "trend up" because of the attention stemming from OCR's enforcement settlements on this issue[2] and perhaps as a result of the pandemic. He reported seeing a marked increase in access complaints in the past five or six months.

OCR's goal is to resolve a "typical" privacy complaint within six months, Haskell said. Cases may need more time because of the pandemic. Haskell noted that he "can't force a privacy officer to go into the office to get all the materials that we need, so that has kind of lengthened it a little."

Describing the process of vetting complaints, Haskell first noted that OCR hears concerns from a variety of sources, including via its online portal and, "still surprisingly," by mail, Haskell said. All go through a "standard review process" to determine if there is a "credible allegation of a violation due to conduct" by a CE or BA, and whether OCR has jurisdiction.

This is "always key because we get a lot of complaints that are filed against noncovered entities," he said, and OCR has no authority to pursue them.

Although OCR may take some complainants at their word, like those who didn't get requested records, typically a

complaint comes with documentation to support claims such as impermissible disclosure. This can include "statements made in court documents, emails, text messages," said Haskell, adding that he has on occasion had phone messages forwarded to him.

"When we start seeing documentation of allegations, that's when we heighten our response," he said. Additionally, any organization with a "checkered past" is going to get more attention. OCR maintains a database on CEs and BAs, and it's the "first thing" that Haskell consults when he begins to work on a complaint.

OCR Aims for Technical Assistance Only

Echoing other agency officials' public comments over time, Haskell said OCR's goal is to achieve compliance through "technical assistance" (TA) versus formal enforcement. If TA fails or OCR believes there are larger problems, an investigative phase, beginning with a data request, will commence.

Given their high caseload, OCR investigators "try and expedite the cases and get them to move as quickly as possible," said Haskell. It would also benefit organizations to resolve matters at the TA phase.

After determining a complaint is valid, OCR sends a TA letter to both the CE and the complainant outlining the allegations along with a "recap of the compliance requirements" related to the allegation.

"I can't stress it enough that covered entities can effectuate compliance a lot quicker than we can," Haskell said. "If you get a letter from us saying we got this complaint, try and take action. A covered entity can take action that day."

Haskell explained that OCR considers a complaint resolved with the issuance of a TA letter. Organizations could contact him about a letter, he said, but it's probably not necessary.

"I don't want to discourage covered entities from contacting me if they ever get a technical assistance letter from me. I want them to communicate with us. But when we issue a technical assistance letter, we close out the case," he explained. "So, there's nothing really to add to the case."

Haskell added that he cannot "field calls on every single technical assistance letter. I would turn into a call center, not an investigator, at that point."

OCR will write a data request letter instead of providing TA and closing a case in some instances.

Investigations Have Three Prongs

Haskell said CEs and BAs are sometimes confused because they fail to realize OCR is "not confined to the four corners of the complaint" and, in fact, has "broad discretion."

Overall, OCR has three goals in its investigations, Haskell explained. First, substantiate the allegation; second, "remedy any harm to the individual"; and third, "identify a root cause."

Some CEs and BAs mistakenly think OCR stops at the second step, and that an investigation is over once the patient gets their records or if workers are retrained about permissible disclosures, for example.

Not so. "If we're ever going to effectuate compliance, we've got to make sure that covered entities are identifying, addressing and resolving the root cause of what caused the noncompliance," Haskell said. "A lot of times it's simply an employee made a mistake, which we understand. There are workforce-sanction policies, and those need to be applied. Or there could be larger issues in terms of incorrect or nonexistent policies and procedures."

For cases that can't be resolved with just TA, the data request letter is designed to uncover these issues. It is not uncommon, for example, for small and mid-size providers to admit they lack policies and procedures for disclosing protected health information (PHI) or for responding to a records request. Having policies that are inaccurate is just as bad as not having any at all.

"I've worked with covered entities where their fee schedule [for medical records access] is completely in noncompliance with HIPAA," Haskell said.

Notification Failures Can Trigger Requirements

Haskell also addressed *RPP*'s question about whether OCR is investigating any cases for lack of notice or late notice following a breach. Haskell was unaware of any such cases that arise solely out of lack of notice, but said he had one where he disagreed with the covered entity's four-factor assessment of whether a breach is reportable.

He noted that the concern is for potential harm in the future, not just whether immediate problems result from a breach. "You want to notify the individual and give them an opportunity to take whatever safeguards and preventive measures that they need to take. You don't get to wait until somebody's Social Security number has been taken" before giving notice, he said.

Haskell said a "more common issue is that there's just some missing elements for breach notification letters."

If there was a failure to give notice, OCR typically would "make you take some action, even though it's outside of the 60 days, and then we're going to get" at why the notice wasn't made within the required time frame.

He said he has required CEs to issue a breach notice letter "six months after the fact" if they had failed to notify patients.

Security Cases Focus on 'Infrastructure'

While most of the cases Haskell discussed involve the privacy rule, he does investigate potential security rule violations. The security rule cases he has been involved in have not yet been resolved and are "still in the investigative process," Haskell said.

Security rule cases take significantly longer than privacy cases. Investigating a security rule allegation "is a very intensive process, and there's a lot of things to try and figure out…a lot of technical things that need to be figured out on both ends. And it's an ongoing process," Haskell said. Security rule investigations also involve OCR subject matter experts who have information technology backgrounds.

While privacy rule investigations may center on issues related to potential "immediate harm" in terms of an unauthorized disclosure or a failure to obtain medical records, a security breach-related investigation will focus more on the infrastructure that was in place at the time, according to Haskell. CEs investigated after a security breach also end up submitting more documents.

"I had one covered entity that…couldn't even figure out if PHI was involved in the breach because as they were trying to get the data from the third-party vendor, the third-party vendor had sent them a file…that was infected. It took them three or four months before they could even get to a point where they could safely download and review the material," Haskell recalled. "Those types of things just don't happen, typically, in a privacy rule matter."

Common among the security rule cases in which he's been involved are a lack of a risk analysis and a failure to act afterward, Haskell said.

Organizations "are running these analyses, identifying vulnerabilities, and then not doing anything to mitigate them," he said. Not only does this expose them to future attacks with ransomware and other threats, but it also increases the likelihood of enforcement action, Haskell said.

"I sometimes think that some entities think that if they just throw enough paperwork at us, that we'll just go away, and the problem is that we want to see the paperwork, but we also want to see the action behind it," Haskell said.

Avoid Becoming a 'High-Impact' Case

A data request letter can "lead to a lot of back and forth" with the investigator, Haskell said. In contrast to receiving calls about TA letters, Haskell said that he doesn't mind when CEs or BAs call him to ask for clarification during a data request or investigation. He said this "saves time" and that he seeks to "build a collaborative relationship" with the organizations.

He noted that OCR's letters include the investigator's name and contact information and that organizations could schedule a phone call. "We can't stay on the phone forever," Haskell said, adding, "I'd rather put 20 or 30 minutes into a phone conversation than put a few hours into more data request letters, getting information I don't need, crisscrossing emails."

But the "biggest issue" he faces is being ignored altogether, which happens more often with small providers, Haskell said.

"I don't care if you give me a one-page response of just actual, absolute nonsense; you just need to respond to us," Haskell said. Of course, he doesn't really want nonsense. In fact, Haskell offered a number of suggestions for how to respond appropriately to a data request letter.[3]

If the responses to the data request indicate the organization has already taken corrective action, "I go into drafting the closure letter," said Haskell.

"Size does matter in terms of how we look at cases, but not from whether or not…a violation has occurred," he said.

"Being a small provider doesn't obviate your compliance responsibilities," Haskell said, adding that OCR recognizes that "a solo provider is going to have a different infrastructure than, say, some of the large entities that we engage with. I've worked with a health care network that had nine attorneys on staff and an internal IT department."

Beyond TA and a simple investigation are what OCR calls "high-impact" cases. These are "moving to enforcement," such as with a resolution agreement. Such cases are deemed to have had a "high impact in terms of harm to individuals," or "potential harm to other individuals if we identify a systemic issue," he said.

Haskell said his "goal is to try and prevent cases from going to high impact" for the benefit of OCR and the CE or BA.

Intner asked Haskell what goes into the decision to enter into a resolution agreement with a CE or BA. Haskell responded that there are "many elements," including the organization's "financial situation," but added that he is "not really privy to those conversations."

Cooperation, Past History Are Key

He noted that, "if we've sent out TA on the same complaint, for the same allegations, you will probably be investigated for that."

Another thing that may trigger an investigation is a negative history with the agency. OCR has "good will" with some CEs, or a "good working relationship," which may spare them from an investigation.

But if an investigator says, "Oh, we're getting these folks again…and we just had a compliance review with them a year or two ago…we're still seeing these issues…we don't feel confident, necessarily, in going forward with TA."

"I can't stress enough that cooperation with OCR goes a long way. We're not going to ignore violations…but our ability to work with covered entities will dictate how we feel best to effectuate compliance when these issues arise," said Haskell.

Particularly with OCR's recent resolutions concerning records access, "you'll see that, probably in at least half of them, there was some contact between the CE and OCR in which the CE didn't respond, either to a technical assistance letter, meaning they didn't take appropriate action, or they didn't respond to our data request letter," he said.

"If I could tell covered entities" and BAs one thing, "it's just respond to us and work with us."

1 John Haskell, "A View From the Inside: A Discussion with an OCR Investigator," Washington, D.C. Regional Healthcare Compliance Conference, Health Care Compliance Association, March 5, 2021, https://bit.ly/2QDgZfM.
2 Theresa Defino, "Does 18th Right of Access Settlement Provide Needed 'Gentle Nudging'?" *Report on Patient Privacy* 21, no. 4 (April 2021), https://bit.ly/3xsEVmO.
3 Theresa Defino, "The Fine Art of Responding to an OCR Data Request," *Report on Patient Privacy* 21, no. 5 (May 2021).