

Report on Patient Privacy Volume 21, Number 8. August 12, 2021 Still Missing a New Leader, Former OCR Directors, Experts Offer Advice, Task List

By Theresa Defino

Issue a final rule revising the privacy regulation and write guidance on the information blocking rule. Formalize the fledgling audit program required by Congress more than 10 years ago. Engage with providers and other HIPAA-regulated entities. And by all means, get cracking.

In a series of interviews with *RPP*, two former Office for Civil Rights directors and a handful of other HIPAA experts weighed in on the tasks that will be facing the new leader of OCR—that is, once HHS or the administration names him or her. Eight months into its term, the Biden administration had not appointed an OCR director, and it's unclear when that will change.

With the pandemic resurging, ransomware attacks escalating and misinformation about “HIPPA” and vaccines entering everyday conversations, the government’s most powerful agency tasked with enforcing medical privacy and security is being led by Acting Director Robinsue Frohboese. While garnering praise for her skills and competence, Frohboese cannot fulfill all the roles of a permanent director, such as launching policy initiatives.

Among those most critical of the lingering vacancy is Roger Severino, OCR director under President Trump who resigned in mid-January, a week before President Biden took office. “There’s no person publicly advocating for HIPAA at the political level, and if you don’t have that voice, then you don’t have the full weight of the administration’s authority behind any initiatives,” he told *RPP*. “And it’s crucially important to fly the flag and explain that [HIPAA] is a priority for the administration.”

Asked by *RPP* to address these criticisms and identify when a director might be named, an HHS spokesperson responded: “We have an acting OCR director, and OCR’s strong commitment to its mission continues forward.”

While the circumstances wrought by the pandemic are unprecedented, it is not so for OCR to lack a new director this far into an administration. Severino was appointed in March 2017, a move that was quicker than under past administrations. For example, Kathleen Sebelius, HHS secretary under President Obama, named Georgina Verdugo OCR director nine months after he took office.

Lingering Vacancy a Surprise

Nearly all of those who spoke to *RPP* said they had expected a new director by now, and none knew why this had not occurred.

Severino said in late July that he “definitely” thought OCR would have had a new director by that time, and accused the Biden administration of “trying to avoid accountability for the changes they are making” by “not appointing somebody as the point person who would be the most directly responsible for what happens in the office. It may be strategic on their part to try to deflect criticism and focus by obfuscating who’s actually in charge.”

Leon Rodriguez, who also served under President Obama before being confirmed as the director of the U.S.

Citizenship and Immigration Services, told *RPP* there was “a lot of motivation and effort to fill not just the OCR slot but political positions throughout the new administration at the beginning” after Biden took the oath of office.

“Once the work of governing began...the momentum seemed to have slowed to fill this position,” Rodriguez added. “I was hearing about interviews and that kind of thing, early on, and I’ve not been hearing about that more recently.” Rodriguez said he could not disclose who might have been under consideration.

Rodriguez called it “important and preferable...to have a full-fledged director in there.” But he also said “there’s a lot of ways in which it doesn’t actually matter.”

The agency “knows what it is supposed to be doing, especially, I think, with respect to HIPAA in terms of just the day-to-day enforcement activity,” said Rodriguez. But he agreed with Severino’s assessment that when it comes to policy initiatives, “it is harder to move forward...if you don’t have somebody in there who is a fully empowered appointee.”

Severino and Rodriguez also shared their firsthand job experiences with OCR.^[1]

NPRM Primary on To-Do List

To the larger question of whether the lack of a permanent director might lull covered entities (CEs) and business associates (BAs) into lax compliance, Kirk Nahra, a privacy attorney and frequent speaker on HIPAA, agreed with others who told *RPP* they were doubtful. “I don’t think there is a material impact on how CEs are acting—these enforcement actions are always a bit slow, and I don’t think anyone thinks they will get a free pass,” said Nahra, partner with WilmerHale in Washington, D.C.

Once a new director comes on board, among the more immediate tasks to be undertaken include writing a final rule to follow up the notice of proposed rulemaking (NPRM) that Severino and then-HHS Secretary Eric Hargan announced on December 10, which didn’t appear in the *Federal Register* until Jan. 21, a day after Biden was inaugurated.^[2]

Severino said the NPRM “shouldn’t be controversial” and expressed the hope that it isn’t “changed or tinkered with much.”

The NPRM, he said, “went through so much analysis and so much deep thought that it was in great shape” when it was published.

Dallas health care attorney Jeff Drummond agreed with the need to finalize the NPRM. He called most of the provisions “anodyne,” and noted that certainty fosters compliance. “I don’t really care if they adopt any of them in particular, just that they make a decision and go with it. It’s hard for us regulatory attorneys to have to guess what the rules will be tomorrow when we are giving advice today,” he said.

Directors’ Audit Hopes Remain Unfulfilled

Both Severino and Rodriguez told *RPP* they wished they’d been able to formalize OCR’s audit program, and that this is something a new director should tackle. Required as part of the 2009 HITECH Act, OCR completed a pilot of 115 on-site audits of CEs from 2012 to 2013, and desk audits of 166 CEs and 41 BAs from 2016 to 2017. It wasn’t until December, under Severino’s watch, that OCR released the results of the audits.^[3] But the agency made no announcements about the future of the program.

Rodriguez described a permanent audit program as “the holy grail none of us quite were able to attain.” This may

require some “rethinking of how you build it and how you test it.” He had hoped to create an audit program that “was well-designed and reasonably well-respected,” but the effort “turned out to be more complicated than I thought,” he said.

An audit program would be useful to elucidate HIPAA violations that now only become known through breach notification. “I think it’s a little bit incomplete for breach notification to be the primary mechanism for detecting violations and promoting compliance,” Rodriguez said.

Audits would “cast a wider net” and would supplement breach notification and complaints as the “primary conduits for enforcement,” Rodriguez said. Audit findings could help promote “truly best practices” on topics such as encryption, and reveal more privacy versus security compliance issues. Such a program could also address allowable and unallowable disclosures, about which he said there is “still of lot of misunderstanding,” particularly when you get away from “big hospital systems and other sort of large institutional providers.”

Severino told *RPP* he would like to see the audit program “converted to more of a traditional audit where the worst actors, the worst violators, for example, those that would not self-report HIPAA violations, which they’re required to do under our regs, would be subjected to a full audit.”

OCR “should recognize the difference between those entities that self-report” and are subject to enforcement actions, versus those that don’t, Severino said, with the latter group receiving more scrutiny. Severino said his “proposal for the future of the audit program [was] to make it more of a traditional audit like an IRS audit, as opposed to what it was historically.”

A Call for Clarity on Info Blocking

Deven McGraw, former OCR deputy director for health information privacy, told *RPP* that recent “federal court decisions undermined some of OCR’s HIPAA regulatory and penalty authorities, and OCR leadership should assess the impact of those decisions and prioritize measures to rectify the damage, which could mean working with Congress on new policies.”

Additionally, OCR “needs to focus more on steps it should take to assure full implementation of the 21st Century Cures Act provisions, including with respect to information blocking,” said McGraw, chief regulatory officer at Ciitizen Corporation, a health information technology and medical records firm.

Specifically, OCR officials “need to better address the intersection of the Cures Act and HIPAA—for example, clarifying whether business associates who are covered by the info blocking rules are ‘excused’ from exchanging data, for example, with patients, if their business associate agreements don’t expressly permit it,” she said.

Nahra and others also expressed what they don’t want to change. Nahra told *RPP* he hoped OCR’s historically “thoughtful” approach to enforcement continues under an incoming director. This “doesn’t mean people get a free pass, but it does mean that the regulators pay attention to whether people are trying and working hard and consistently improving. That is important as the health care system evolves,” he said.

A new director, said Nahra, should “resist the cheap enforcement that occasionally comes from other agencies.” Noting there are “significant reasons in the health care system to make sure that data is shared for positive purposes,” Nahra said “too aggressive enforcement will threaten that.”

Need for ‘Certainty,’ Ransomware Guidance

Drummond recommended that OCR continue an initiative like Severino’s records access program, saying he’d “rather see a hundred \$10,000 fines than one \$1 million dollar fine, because I think it focuses the attention of the

regulated class much better.”

But he suggested that OCR officials find a new target about which “they are getting a lot of complaints,” which could, for example, include violations involving email, texting or snooping by employees.

Rodriguez pointed out that ransomware and hacking attacks weren’t much of a threat or a reality during his tenure, certainly not like they are today.

For the new director, “ransomware is going to continue to be a big issue,” Rodriguez said. OCR needs to “educate providers on how they protect themselves and how they prepare to recover when they are the victim of a ransomware attack.”

Contact Severino at rseverino@eppc.org, Rodriguez at lerodriguez@seyfarth.com, Nahra at kirk.nahra@wilmerhale.com, Drummond at jdrummond@jw.com, and McGraw at deven@ciitizen.com.

1 Theresa Defino, “What Does it Take to Run OCR?” *Report on Patient Privacy* 21, no. 8 (August 2021).

2 Theresa Defino, “On the Eve of a New Administration, OCR Offers ‘Comprehensive Reforms’ to HIPAA,” *Report on Patient Privacy* 21, no. 1 (January 2021), <https://bit.ly/3op12Vr>.

3 Theresa Defino, “Belated OCR Audits Shine New Light on Old Issues, Including Security Failures,” *Report on Patient Privacy* 21, no. 1 (January 2021), <https://bit.ly/3ly5SlB>.

This publication is only available to subscribers. To view all documents, please log in or purchase access.

[Purchase Login](#)