HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Right of Access Initiative Yields Major Settlements with OCR

The HHS Office for Civil Rights (OCR) announced that it has settled five more investigations in its HIPAA Right of Access Initiative, an enforcement priority intended to support the right to timely access to health records at an affordable price.[1]

All the settlements stemmed from patients or family members complaining a healthcare organization had not responded appropriately to requests for patient records. OCR issued guidance on access rights in 2016, advising hospitals and other HIPAA-regulated entities regarding the expectations and requirements inherent in the patient's right to access of his or her PHI in the designated record set (DRS).[2]

The DRS is the body of information used to make decisions about the patient's care or payment for care. In 2019, OCR launched the enforcement initiative that resulted in these most recent settlements.

"The OCR means business," says **Sarah E. Coyne**, JD, partner with the Quarles & Brady law firm in Madison, WI. "Rumor has it that additional guidance or regulations will be issued imminently in light of the *Ciox* decision relating to third party requests for electronic PHI and appropriate parameters including fees, which changed the access landscape."[3]

Coyne notes the HIPAA Right of Access Initiative may receive a boost from the concurrent requirements under the Office of the National Coordinator for Health Information Technology (ONC) information blocking rules.[4] Both provide a basis for legal action against those who stand between patients and their medical records.

Much confusion remains about when healthcare entities can and cannot release information under HIPAA, says **Kim Stanger**, JD, partner with Holland & Hart in Boise, ID. The confusion is most common among smaller physician practices and similar healthcare operations, he says. "Part of the risk manager's job is to identify and correct those misunderstandings," Stanger says. "Some people still think that if a patient requests information that was obtained from another hospital or provider, the hospital can't provide that information to the patient. That's not true under HIPAA."

> MUCH CONFUSION REMAINS ABOUT WHEN HEALTHCARE ENTITIES CAN AND CANNOT RELEASE INFORMATION UNDER HIPAA.

Similarly, healthcare workers may think HIPAA prevents providing lab results because they must be provided directly from the lab, or that parents may not obtain patient information even if they are the personal representative under HIPAA.

"It's very easy for the medical records offices to adopt these false beliefs. They get lax and don't follow up on anything they're not sure about," Stanger says. "OCR is demonstrating that this is not acceptable and that healthcare organizations must provide the proper training and support for the people in your organization who make these decisions."

Coyne says there are some lessons to be learned from the enforcement initiative and how the enforcement initiative has played out to date:

- The patient has the right to all the PHI in his or her DRS, no matter how old it is, where it is stored, or where it originated.
- There are few circumstances in which OCR will decide it was justified for a hospital to provide access to a

patient who requests it. For example, if the basis is the information was not used for making decisions about the patient, the hospital must be able to support that justification.

• The hospital can require the request to be in writing but cannot create an unreasonable barrier. For example, it cannot require the person to come to the hospital health information management department in person.

• Patient complaints matter. The settlements have been prompted by patients complaining to OCR that they could not access their medical information in a timely fashion.

• Timing matters. Hospitals that take longer than the prescribed 30-day timeline (plus a 30-day extension) risk penalties. The period may be more restrictive under state law. Hospitals should rigidly adhere to these timing parameters. The settlements show OCR is willing to penalize even short delays beyond those timelines.

• It is a good time for hospitals to review and update their right to access policies, although new guidance may be imminent and will need to be incorporated quickly upon release.

• Covered entities should ensure their business associates are aware of the access enforcement initiatives and are up to speed in the associated requirements.

• Hospitals must not charge excessive fees. HIPAA allows a reasonable cost-based fee, subject to state law, and no search or retrieval fees, regardless of state law.

• Cooperating with OCR is required — and a good way to try to mitigate the size of the penalty/settlement.

The settlements from this initiative should not be surprising, says **Alisa L. Chestler**, JD, CIPP/US, shareholder with Baker Donelson in Nashville. The process includes many moving parts, so healthcare organizations sometimes stumble when responding to records requests, she says.

"In our mobile world, people are used to having information at their fingertips. They see no reason that their medical information should be any different. Patients know the information exists electronically and, therefore, want to have what they need," Chestler says. "Frankly, this is also more a matter of who is complaining, as many of the complaints come from the patient's lawyers looking for the information on the patient's behalf. They know that many times the providers, especially the smaller providers, are not equipped to handle such requests quickly or efficiently."

Still, most cases are a lesson in what not to do, Chestler says. Many initially were contacted by OCR and given "technical advice" with an intention to close the matter, she notes. However, the providers did not send the records even after the technical advice, and the OCR likely was frustrated with their inaction and noncompliance. Aside from the monetary penalties, each has either a one- or two-year monitoring period, which is an expensive and onerous process.

"What was most interesting about many of the cases is that they appear to be in specific areas in which there might have been more complex issues, including mental health, substance abuse, and minor records," Chestler says. "Providers should know in advance their understanding of the state laws and be able to react quickly and appropriately. The laws surrounding minors, custodial parents, and related issues can be particularly complicated. Providers should have at least a baseline understanding of the issues so they are prepared." ■

REFERENCES

1. HHS.gov. OCR settles five more investigations in HIPAA Right of Access initiative. Sept. 15, 2020. https://bit.ly/34UO3Ez
2. HHS.gov. Individuals' right under HIPAA to access their health information 45 CFR § 164.524. Content last reviewed Jan. 31, 2020. http://bit.ly/2RzGD2X
3. *Ciox Health, LLC v. Alex Azar, et al.* https://bit.ly/3p7OZ0u
4. HHS.gov. HHS extends compliance dates for information blocking and health IT certification requirements in 21st Century Cures Act final rule. Oct. 29, 2020. https://bit.ly/2I5uJeC

Ongoing Noncompliance Leads to Serious Settlement for Small Clinic

An orthopedic clinic in Georgia has agreed to pay $1.5 million to OCR and to adopt a corrective action plan to settle potential HIPAA violations the government said amounted to systemic noncompliance.[1] The clinic serves about 138,000 patients per year, and it is significant that OCR came down hard on a relatively small player.

A reporter contacted the clinic to inform staff that a database of patient records may have been placed online for sale. Shortly thereafter, a hacker contacted the clinic demanding ransom in exchange for a complete copy of the stolen records. Clinic staff learned the hacker used a vendor's credentials to steal the information. In its breach report, the clinic noted more than 208,000 patients were affected.

"OCR's investigation discovered longstanding, systemic noncompliance with the HIPAA Privacy and Security Rules," OCR reported. Those included "failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with multiple business associates, and provide HIPAA Privacy Rule training to workforce members."

The growing risk of cyberattacks may have caught up with the clinic, says **Matthew R. Fisher**, JD, partner with Mirick O'Connell in Worcester, MA. The original incident occurred in 2016, but the parties settled this year.

"This case goes back a few years, so maybe scope of the risk from an outside cyberattack wasn't quite as appreciated as it would be now," Fisher offers. "Nevertheless, this is consistent with cases where we see an incident that gets OCR's attention, and then there is broader noncompliance in the background. No risk analysis is very bad from the government's perspective, given all the clear guidance provided. If you're not doing that, there is going to be a lot of unhappiness with your operations."

It also is important to take cyberattacks seriously and respond quickly. It appears the Georgia clinic may not have acted swiftly. The clinic also may not have been monitoring online sites for data stolen from its system, since a reporter alerted the clinic to the problem.

"The lesson is you always have to be monitoring your systems and doing what you can to figure out what's been going on," Fisher stresses. "You don't want to be in that scenario where you're relying on someone else to tell you your system has been compromised."

This case demonstrates how HIPAA is one of the rare laws where one earns credit just for trying, says **Mark R. Ustin**, JD, partner with Farrell Fritz in Albany, NY. It is the failure to make that minimum effort that lands covered entities in trouble, he says.

"The things that got them in trouble are all the very basic things, whereas in a lot of other legal situations you can run afoul of complicated requirements that can trip up anyone," Ustin explains. "This was all extremely avoidable. Someone might ask how OCR is holding them responsible for someone hacking into their system and stealing data. When you look at their obligations and what they failed to do, it becomes clearer why this penalty was applied."

Systemic noncompliance only comes into play when a covered entity has failed to take the most basic measures to comply with HIPAA, usually over time. It is not a charge that comes from merely overlooking one detail of the requirements.

Unfortunately, systemic noncompliance is not uncommon, Ustin says. In some cases, entities do not realize their data are subject to HIPAA requirements, such as when business associates fail to protect PHI.

"Once that happens, that is when you've opened the door to having a systemic problem," Ustin adds.

The central OCR finding regarding the clinic's breach was "longstanding systemic noncompliance," notes **Sarah E. Coyne**, JD, partner with Quarles & Brady in Madison, WI. The term "systemic noncompliance" has become something of an OCR buzzword, she says.

The entity had violated multiple parameters of HIPAA for a long time, including those that are focus areas for OCR (e.g., the requirements for risk analysis, audit controls, and business associate agreements).

"Although there is enforcement discretion currently in play regarding telehealth-related disclosures until the end of the national public health emergency, OCR is not hesitating to bring down the hammer in other circumstances," Coyne says. "In addition to its vigorous enforcement of the right to access standard, OCR has had it with longstanding widespread noncompliance. This case shows us that the penalties are

not reserved for large health systems only."

When OCR receives a breach report involving 500 or more individuals, the agency is obligated to investigate, Coyne says. It looked into the breach that was reported, but this case illustrates how OCR also will explore the past, regardless of whether that is directly related to the current breach.

"The [Georgia] case also teaches us that OCR views hacking through a lens of whether the covered entity did enough to guard against it," Coyne says. "Specifically, if an entity is hacked, it should be able to demonstrate compliance with the privacy and security rules through audits, risk analyses, updated policies, and training."

To guard against enforcement actions, hospitals should evaluate their policies to ensure they are up to date. Perhaps even more importantly, hospitals should examine all their vendor contracts and ensure there are business associate agreements in place. Business associates must be aware of their own direct responsibility under HIPAA, and they must put their own policies and training in place.

"The risk analysis is not theoretical. It is required, and it is a big deal for OCR," Coyne says. "Hospitals should ensure they are doing regular and proper risk analyses, which may require third-party contractors to do a full gap analysis, and then it is vital to address the deficiencies identified."

The settlement with the clinic was the ninth settlement of an alleged HIPAA violation this year, and the OCR has since settled four more investigations, notes **Erin Dunlap**, JD, an attorney with Coppersmith Brockelman in Phoenix. This one is particularly noteworthy, she says, because patient records were made publicly available online for sale, a journalist discovered the issue, and the records contained sensitive information, including Social Security numbers, medical procedures, and test results.

"No doubt this made for a bad combination in the eyes of OCR. Like many other providers subject to an OCR investigation, the clinic didn't fare well, particularly on the security side," Dunlap says. "The HIPAA Security Rule has been around for almost 20 years and is intended to be flexible based on the size of the organization. However, healthcare providers, particularly smaller ones, are still lagging and lacking from a security standpoint, as cyber risks are on the rise."

The risk analysis, which can be conducted internally or by an outside vendor, is the critical first step in meeting the HIPAA security requirements, Dunlap says. If an organization is subject to HIPAA and has never performed and documented a risk analysis, it is important to complete one.

If resources are limited, Dunlap advises using the Security Risk Assessment tool provided by OCR.[2] Prepare a corresponding risk management plan for correcting or mitigating the risks that were identified in the risk analysis.

"Those two steps, even if imperfect, will help any organization if they are hit with an OCR investigation. In fact, OCR almost always requests those two documents ... even if the incident that triggered the review did not involve a security issue," Dunlap says.

Dunlap notes the Georgia clinic is now subject to a two-year corrective action plan (CAP) as part of its resolution agreement with OCR.

"Not surprisingly, one of the first tasks under the CAP is to perform a risk analysis, and OCR is overseeing that process," she says. "It's certainly better to get it done before the government comes knocking." ■

REFERENCES

1. HHS.gov. Orthopedic clinic pays $1.5 million to settle systemic noncompliance with HIPAA rules. Sept. 21, 2020. https://bit.ly/38cU3uc
2. HealthIT.gov. Security Risk Assessment Tool. Content last reviewed Sept. 14, 2020. https://bit.ly/2HVEcWt