Podcast Transcript

2022 DSIR Deeper Dive: OCR's Right of Access Initiative

Date: November 16, 2022

Guest: Courtney Litchfield and Lynn Sessions, **Host:** Amy Kattman

Run Time: 19:31

For questions and comments contact:

Courtney L. Litchfield

Associate
Chicago
T: 312.416.6236 | clitchfield@bakerlaw.com

Lynn Sessions

Partner
Houston
T: 713.646.1352 | lsessions@bakerlaw.com

Kattman: Ransomware. MFA. Extortion. Fraudulent fund transfer schemes. These topics and many others make up the key findings section of the 8th Annual Data Security Incident Response Report, informally known as the DSIR Report. Each year, the incident response attorneys within the Digital Assets and Data Management Group, or DADM, provide statistics and analytics around the incidents they encountered the previous year in a report that is eagerly received by clients, vendors, media outlets, and, frankly, anyone interested in or tasked with their company's digital asset and risks. I'm Amy Kattman, and you're listening to BakerHosts.

This, our 10th episode in the series exploring the 2022 DSIR report, is focused on the Office for Civil Rights, or OCR's Right of Access Initiative. Our guests today are Courtney Litchfield, an associate in our Healthcare Privacy and Compliance team, and Lynn Sessions, partner and leader of the Healthcare Privacy and Compliance team. Welcome to the show, Courtney and Lynn.

Litchfield: Good morning, Amy. Thank you for having us.

Sessions: Happy to be here.

Kattman: Let's start from the beginning. Lynn, can you tell us what is the Right of Access Initiative, and what does it stem from?

Sessions: So, the Right of Access Initiative stems from the HIPAA privacy rule, and the HIPAA privacy rule outlines both the rights that patients, or individuals as it is sometimes referred to in HIPAA, that they have, as well as the duties and obligations that covered entities and business associates have to provide. So at the center of the OCR's initiative is the right of a patient or a patient's personal representative, so sometimes their agent it is referred to, to access their medical records in a timely and a cost-effective way. OCR created this Right of Access Initiative to help support these rights.

Several years ago, we worked with several healthcare entities, covered entities, on OCR investigations. The OCR had been receiving complaints from patients and sometimes their attorneys, claiming that they were not getting the records that they had requested, or they were being charged too much for those records. There were some state laws in effect at the time, and some of them are still on the books, that allow for healthcare entities, physicians, and hospitals, and others to charge for the copying of medical records. And so many of our clients were actually following those state-mandated costs. The OCR came back and said nope, you're charging too much. There is nothing but a reasonable cost, a cost base that you can actually charge patients to receive copies of their records. This resulted in specific guidance from the OCR on how to provide the records and to whom, the time frame for doing so, and the cost that could be associated with them.

So when the new administration came in in 2016, there was an all-out initiative for patients to have access to their records, really, anywhere at any time, with personal health records, health information exchanges, electronic medical record portals and apps for your phone so that you can get access to your medical records anywhere, anytime. With that came many of our clients receiving what is called technical assistance from the OCR and/or investigations from the OCR on their policies and procedures for the release of medical records and a focus on any burdens to patients, especially during the pandemic. So, whether it was the completion of a specific form or if it was a cost associated with receiving those medical records, that would go to the patients or their agents to receive, and readily receive their medical records. Thus far, this has continued on with the new administration following the election in 2020. Courtney, anything you'd like to add to that?

Litchfield: Sure, yeah. I'll just note that OCR refers to HIPAA's Right of Access as a fundamental right. So, typically when you hear the phrase fundamental right, you might think of the Bill of Rights outlined in the United States Constitution, the right to vote, freedom of speech. And the fact OCR is leveling a patient's right to access their medical information with these other fundamental human rights really underscores how important this initiative is to OCR.

Kattman: Thank you. Courtney, as a healthcare provider, what are the main points to keep in mind when responding to a Right of Access request?

Litchfield: The Privacy Rule outlines various standards and implementation specifications with respect to an individual's right to access their medical information. There are a lot of nuances with these provisions, and we, of course, do not want our listeners to fall asleep, so I'll keep this fairly high-level and touch on some of the more just big-picture items.

The first big one is scope, and the question there is what does a patient, or their legal representative or another permissible third party, actually have the right to access? And the answer is the designated record set. What is a designated record set? That is the next question, right? So this includes all identifiable patient information that is created, received, maintained, used by a provider in the course of treatment. There are two buckets that are expressly excluded from this definition, and that is psychotherapy notes and information that is compiled in anticipation of litigation or a similar type of proceeding.

Next is timing. Providers are expected to respond to an individual's request within 30 calendar days. Not business days. Calendar days. This response must either be the provider fulfilling the request, so sending the requested records or provisioning the requested access, explaining why they are denying the request, or informing the individual that they need up to 30 additional days to fill the request. This isn't probably or at least 30 more days. It is at most 30 more days. While this seems fairly straightforward, it is actually one of the provisions that many providers often fail to meet.

Then there are other provisions that are a bit more complicated since they vary depending on who is requesting the access. For example, there are certain limitations on the fees a provider can charge as Lynn mentioned earlier. So, for example, if patient Lynn Sessions reached out to her provider ABC Healthcare asking for access to her information, HIPAA's fee limitation would apply. However, if I, Lynn Sessions's amazing, smart, awesome lawyer, reached out to ABC Healthcare asking for copies of her records, these fee limitations would not apply. They could charge me a fee. A similar varying provision is with respect to, like a written authorization. So again, if Lynn wanted her records from her ABC Healthcare provider, they don't necessarily need to require that she put this request in writing or sign an authorization. On the other hand, if I, again, Lynn's amazing lawyer, reached out to ABC Healthcare, then HIPAA would require that they obtain a signed, written authorization from Lynn. Lynn, do you have anything to add to that?

Sessions: Well, other than the fact that you are my amazing lawyer, I would say I just want our listeners to note that, HIPAA is really just a baseline for compliance in this particular space. In other words, HIPAA does not preempt state law that provides individuals, patients, others with a greater right of access to their protected health information. This is important to keep in mind, especially as it relates to a time frame in which a provider has to respond to produce records, as well as the fees, as we've talked about, that they're able to charge. So for example, here in my

home state of Texas, licensed physicians are expected to respond to a patient's access request within 15 business days that they receive that request. HIPAA allows for 30 calendar days. So you can see that is a greater right that an individual here in Texas has. So HIPAA does not preempt that. You still have to follow state laws if you're in the state of Texas for this particular provision.

Another example that we've talked about already, is the fact that state laws do allow for the charging of fees for records. Sometimes it is on a per-page basis, sometimes it is for the collection of records and HIPAA specifically prohibits the provider from charging anything other than a cost-based reasonable fee when the provider is producing the records to a patient. So even if it is permitted by state law, that is something that is specifically prohibited by HIPAA.

Kattman: Since 2019, there have been 41 publicized resolutions related to Right of Access claims. Courtney, can you give us a brief summary of enforcement actions to date?

Litchfield: Sure. So the 41 enforcement actions consist of two civil monetary penalties, or CMPs for short, and 39 resolution agreements, often referred to as a settlement. So, altogether across those 41, OCR has obtained over $2.4 million. In 2019, OCR announced this initiative, and that year they also announced two resolution agreements. So while there wasn't much action from OCR in 2019, again, that is when they first kicked this initiative off. Jump to 2020 and just over 50% of these, of the enforcement actions announced that year, related to the Right of Access Initiative. In 2021, this figure went up to 85% with 12 of the 14 enforcement actions involving a patient's right of access to their medical information. So far this year, while the number of enforcement actions is higher than any previous year, we're currently at 16, we are still on par with 2021 because the 16 that have been announced makes up about 80% of the enforcement actions announced by OCR overall for this year to date.

While 2022 is coming to a close, it is very possible we see more action from OCR in this area. So, backing up, typically OCR will announce an enforcement action one at a time. However, with this Right of Access Initiative, OCR started a trend where they're announcing anywhere from four to even 11 enforcement actions at once. So we could see that 16 number increase in the less than two months we have left in the year. Lynn, what do you think?

Sessions: So I can tell you that we were reached out to, particularly during the pandemic, from clients of ours who'd received proposed resolution agreements and corrective action plans. We've counseled a number of clients over the years on not only the investigations, even when they've received technical assistance or multiple technical assistance, and wanting to know if there is something they should do about it. But when resolution agreements came in, they certainly sought our guidance on how best to respond. And they did come in to a variety of different clients, kind of in a collective manner. We were handling, at the end of 2020, we were handling probably four of these, all at the same time, from different clients in different regions of the country.

One of the differences, just so that the listeners are aware, between a civil monetary penalty and a resolution agreement, as Courtney mentioned, a resolution agreement is really a settlement. It is a settlement that the entity reaches not only with a dollar amount but also with a one- to two-year, that we've seen in this context, a one- to two-year corrective action plan. CMPs are imposed when the OCR can't reach an agreement through the covered entity's demonstrated compliance or their refusal to enter into a resolution agreement and corrective action plan with them. The two CMPs issued under the Right of Access Initiative occurred when the covered entities just completely failed to respond to the OCR's continued requests. At least that is what was reported by the OCR in their press releases.

I think that is something else that is important to think about, too, is not only will you enter into these resolution agreements and corrective action plans with the OCR, which there is a cost associated with a one- to two-year corrective action plan for many of our covered entities, but there is also a press release that gets issued by the OCR on their website. And it is oftentimes picked up by some of the healthcare industry magazines such as Modern Healthcare or Becker's, things along those lines. We see clients become a little bit nervous about the reporting of that in the media.

Kattman: So, looking at these enforcement actions, Courtney, what do you see as the themes and enforcement approach?

Litchfield: Yeah, just quickly to note a minor caveat for listeners that may not be as familiar with what OCR makes publicly available with respect to these enforcement actions. So we'll typically see a press release, and then as Lynn noted, we'll have the resolution agreement, or if it is a CMP, a notice of proposed determination. These materials are fairly high level and do not provide granular specifics or the nitty gritty details about like what happened. But they generally do give us enough information to understand at least the order of events and the violation or violations that contributed to the enforcement action.

So when looking at all 41 together, the most consistent violations highlighted in the available materials include a failure to provide access to a patient's legal representative, so a parent, for example, or another third party like a lawyer; taking well over 30 days to respond to a request; charging a flat fee; or denying a patient's request until they pay off their outstanding balance. That last one is not a consistent violation, but it is my personal favorite, so I had to mention it.

What I think stands out the most is the significant decrease in the number of times OCR provided technical assistance and closed a matter before moving to initiate a formal enforcement action. So, like Lynn said, technical assistance, it comes in the form of a letter, summarizes the complaint and covered entity's response, explains patient's right of access under HIPAA, and then provides that covered entity guidance on how to comply. Technical assistance administratively closes OCR's investigation, and they're generally welcomed with open arms by covered entities that are the subject of an investigation.

So looking back at those 11 enforcement actions in 2020, OCR issued technical assistance over 50% of the time. So in other words, it wasn't until OCR received a second complaint from the patient stating that they still have not received their records and OCR opened another investigation that they then eventually initiated a formal action. So as of 2020, providers may have thought that they would get at least one get-out-of-jail-free card. But in 2021, OCR issued technical assistance less than one-third of the time. And so far this year, in 2022, OCR has issued technical assistance only once. So again, the materials OCR makes available do not provide all of the details, so this does not mean providers subject to a Right of Access complaint should expect a fine. However, it should make providers prioritize and of course, as needed, refine their processes just to ensure they are complying with the patient's right of access. Lynn, do you want to touch on OCR's approach to enforcement?

Sessions: Sure. So in discussions with OCR, just to reiterate what Courtney said, sometimes these corrective action plans and resolution agreements are proposed after OCR has provided multiple, multiple technical assistance to a specific entity, right? And some of that is not getting reported by the OCR even when a resolution agreement corrective action plan is entered into. What the corrective action plans typically look like, as I mentioned earlier, they last about one to two years and will often include and require revisions to policies and procedures that then have to be approved by the OCR; training to your entire workforce, we've been successful in limiting the training to the people who really need to know this information; annual reporting requirements to the OCR for similar types of incidents or if there has been a violation of the policies and procedures; and things along those lines.

One of the things I would like to caution our covered entity clients and business associates with is that when you receive technical assistance from the OCR to please take it seriously. If there are instructions in there to revise your policies and procedures, do that. Look at the policies and procedures around release of information because that can help prevent a potential resolution agreement corrective action plan that the OCR may ask you to enter into at a later date. If the covered entity can demonstrate that they've already made the revisions to their policies and procedures, trained the appropriate personnel in this particular area, then they may be able to avoid an enforcement action. Sometimes these investigations find other HIPAA violations relative to safeguards and things along those lines, so it is not unusual for the OCR to kind of open up your entire HIPAA program. But one of the things we have found with the Right of Access investigations is that they do tend to focus just on this particular part of the privacy rule.

Kattman: As we wrap up our discussion, Lynn, what do you think we can expect with respect to the Right of Access Initiative as we move into 2023 and beyond?

Sessions: So this is a carryover from the prior administration. There is no doubt about that. We expect the Right of Access Initiative to continue under the current administration, in particular with the OCR's top enforcement priority continuing on. One reason for this is because of the Notice of Proposed Rulemaking that the

OCR issued in 2020. With respect to an individual's right of access, proposed changes to HIPAA include cutting the response time frame in half for a covered entity to provide their medical records. Covered entities will be expected to act on access requests within 15 calendar days instead of the current 30 days. Allowing individuals to inspect their records in person and take pictures, videos, and notes of those records while they're there. Allowing individuals, patients and others to direct a covered entity to transfer PHI to a personal health record application that is used by the individual. And again, this kind of goes back to what I said earlier, they want patients to have access to their records anywhere, anytime, regardless of who the provider is that is providing their care.

The date that the final rule would be published and when organizations subject to HIPAA will be expected to be in compliance is yet to be announced. With the 21st Century Cures Act and information blocking, the final rule sought to eliminate intentional barriers to access to medical records, exchange of health information, and the use of health information by giving patients greater control, almost complete control over their personal health data and making it easier to share patient records between organizations and with patients. The idea behind this is that an individual should have access to all of their personal health information anywhere, anytime. And I don't see that changing just with the change in administration in Washington.

Kattman: Thank you, Courtney and Lynn, for this valuable information.

Litchfield: Thank you so much for having us on BakerHosts.

Sessions: Thanks, Amy.

Kattman: If you have any questions for Courtney and Lynn, their contact information is in the show notes. As always, thanks for listening to BakerHosts.