Interestingly, Pitman said, the court didn't take a stance on whether the HIPAA violation creates a breach of contract. "They instead found that there just wasn't an injury," she explained. "They never really made that decision."

All the claims raised by the plaintiff were state law claims, so there wasn't any decision regarding whether there might be a HIPAA violation or a violation of Federal Trade Commission (FTC) health privacy rules, Pitman said.

"The plaintiff alleged a common law privacy claim, and he also alleged that the combination of data with the medical records alongside the geolocation and demographic data collected by Google independently through a smartphone app created a perfect formulation for re-identification of data," Pitman said. "The court found that this was really a hypothetical risk. There was no allegation that this actually occurred or that it would actually create a risk of re-identification for the data."

Take-home messages for privacy professionals include the fact that the court rejected speculative claims, and "the data holder was not held accountable for merely possessing the data or allegedly having the ability to re-identify the data," Pitman said. "The court made it fairly clear that there needs to be some sort of bad intent or actual bad act that occurred at the same time, an actual intent to re-identify the data."

Explain Data Uses to Patients

The use of AI in health care is evolving and likely will continue to grow and develop over many years, Pitman said.

"The decision underscores the importance of having a HIPAA-compliant notice of privacy practices and authorization and making sure that adequate notices are given to patients to explain what information is collected, how the information is processed and what information may be used for," she said. "So, this is probably a good time for health care providers in general to review their notices of privacy practices and authorizations and determine if they are making correct and appropriate disclosures."

Hartsfield also cautioned against looking at the case "as a precedent for being able to use limited data sets for AI without taking a careful look at other aspects of the case." She noted that the HHS Office for Civil Rights still can investigate, as can the FTC. "And so, the lower court raised some important questions, particularly about whether this whole deal was a sale of protected health information," which is prohibited in most cases without patient authorization, she said. One of those exceptions allows providers to sell PHI for research purposes but only for a "reasonable cost-based fee," she said.

"The [district] court actually found that the plaintiff's claim that the PHI was improperly sold was on firm ground," she said. "The court observed that the license that the hospital got to use these trained models and predictions was indirect compensation, and the court noted that remuneration doesn't have to be money; it can be an in-kind exchange. Google didn't explain why this exchange of PHI for the right to use these models was the equivalent of a reasonable cost-based fee rather than direct or indirect remuneration that would require patient authorization. It was still a sale, arguably, even though the disclosing entity retained the ownership rights to the data."

In part due to the lower court's 2020 opinion, Holland & Knight now includes a clause in its model notices of privacy practices saying that written permission will be obtained for the sale of PHI, except if HIPAA permits it, Hartsfield said. "And I'm hopeful that a court would say that 'except if permitted by HIPAA' language would give us enough flexibility there to do things that HIPAA does allow and that aren't a sale," she said. ✧

Endnotes

1. Dinerstein v. Google, LLC, United States Court of Appeals for the Seventh Circuit, No. 20-3134, https://bit.ly/3Qm1mo2.
2. Beth Pittman and Shannon Hartsfield, "Artificial Intelligence in Healthcare and How to Comply with HIPAA and State Privacy Laws," Holland & Knight, podcast, 24:26, October 5, 2023, https://bit.ly/3FNjHoU.
3. Dinerstein v. Google, LLC, 484 F.Supp.3d 561 (2020), https://bit.ly/47dKC9g.

All OCR Enforcement Waivers Expired; Are Your Telehealth Services HIPAA Compliant?

Aug. 9, at midnight. This is the date and exact time the HHS Office for Civil Rights (OCR) ended its HIPAA enforcement discretion for the use of telehealth—giving itself back the authority to enforce portions of the privacy, security and breach notification rules it had let slide during the pandemic. In May, OCR ended the three other enforcement waivers, 30 days after the COVID-19 public health emergency (PHE) was declared over.

So, now that fall is here, covered entities (CEs) and business associates (BAs) are all in full compliance with all relevant HIPAA regulations that were loosened for telehealth and other activities during the pandemic, correct?

Not sure? Perhaps now is an appropriate time to *be sure.*

Beginning in 2020, OCR issued four enforcement discretions that allowed CEs and BAs to undertake some activities in ways that might typically violate HIPAA but which OCR officials believed were necessary in light of the COVID-19 pandemic to speed up care and treatment and help end the virus.

On April 13, OCR declared in the *Federal Register* that with the May 11 expiration of the PHE, OCR's enforcement discretions would also expire—except when it came to telehealth.[1] For telehealth, OCR allowed an extra 90 days for a "transition period" related to the "provision of telehealth using non-public facing remote communication technologies." This is the timing that led to the Aug. 9 compliance deadline.

"During the 90-calendar day transition period, OCR will continue to exercise its enforcement discretion and will not impose penalties on covered health care providers for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth," OCR said in the *Federal Register*. "These regulatory requirements remain the same as they were before the COVID–19 PHE; however, OCR recognizes that regulated entities that began using remote communication technologies for telehealth for the first time during the COVID–19 PHE may need additional time to come into compliance."

Trio of Waivers Expired in May

To review, OCR's three enforcement discretions (aside from the one for telehealth) addressed the following activities. As of May 11, all appropriate HIPAA safeguards should now be in place for:

- uses and disclosures of protected health information (PHI) by BAs for public health and health oversight activities in response to COVID-19.
- "good faith participation in the operation of COVID–19 specimen collection and testing sites," which include "mobile, drive-through, or walk-up sites that only provide COVID–19 specimen collection or testing services to the public." This discretion was applicable to "covered health care providers, including some large pharmacy chains, and their business associates, in connection with the good faith participation" in collection and testing sites.
- "online or web-based scheduling applications for the scheduling of individual appointments for COVID–19 vaccination during" the PHE. Such applications are "non-public facing online or web-based" and allow for "appointments for services in connection with large-scale COVID–19 vaccination."

When it came to telehealth, OCR said CEs might need the extra time to choose "a telehealth technology vendor that will enter into a business associate agreement and comply with applicable requirements of the HIPAA Rules." It also reminded CEs to "review and update as necessary any policies and practices developed and implemented prior to the COVID–19 PHE for compliance with the HIPAA Rules."

'Immediate Steps' Include Scrutiny of BAs

Shortly after OCR announced the impending end of the PHE and its enforcement discretions, attorneys Dianne J. Bourque and Lara D. Compton with Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C., felt CEs and BAs probably needed help unwinding any activities they might have begun during the pandemic that were no longer going to be allowed, or which needed changes to become HIPAA compliant. Their extensive blog post outlined a series of compliance steps to be taken by entity; CE, BA and subcontractors are discussed.[2]

They stressed that "vendor due diligence" and a security assessment were priority tasks CEs and BAs should have undertaken when they learned the PHE was ending. Speaking generally and without addressing telehealth directly, the attorneys cautioned in their post that "all HIPAA regulated entities need to quickly come into compliance and should:

- "identify BAA [business associate agreement] needs and begin applicable negotiations as soon as possible;
- "conduct due diligence on vendors relating to privacy and security requirements;
- "conduct security risk assessments and update risk management plans and security policies and procedures accordingly; and
- "train employees on what the end of the PHE means from a HIPAA compliance perspective."

In addition to their post, the Mintz attorneys jointly answered questions from *RPP* via email.

"We counseled a number of HIPAA-regulated entities throughout the pandemic, including advice on pivoting to telehealth services" during the enforcement discretion pause, Bourque and Compton told *RPP*. "It was strange at that time to advise clients that ignoring certain HIPAA requirements was permissible, and we had concerns about how those clients would later come into compliance, especially if the pandemic was of lengthy duration, which it was."

To them, the extra 90 days for telehealth compliance "made sense since the vendor due diligence and contracting process takes time, as does the implementation of new technologies if needed, and it may take certain organizations longer to go through these steps if they are lacking resources coming out of the pandemic."

Bourque and Compton added that it also takes time to "change the workforce's culture around HIPAA and to retrain employees who likely got used to doing things a certain way during the [PHE] and now have to approach their jobs differently."

The attorneys pointed out that "telehealth does increase certain privacy and security risks, for example, the complexity of telehealth platforms and the ability to participate in a session from anywhere increases the likelihood that a conversation could be overheard or that

records could be generated and stored in offsite locations presenting unique security concerns."

'Expedited Onboarding' May Have Led to Issues

Bourque and Compton said that, in their "experience, it seems that telehealth providers are more likely to engage with vendors that do not exclusively support health care providers, perhaps due to communications technology needs. So, the risk of business associate non-compliance often seems heightened in the telehealth context." These concerns "could be addressed by conducting vendor due diligence and a security risk assessment," the attorneys said.

One "struggle" their clients have faced is signing new BAAs. "It's always a challenge for a regulated entity to ensure that appropriate business associate agreements are in place in advance of a relationship, but the idea of going back and negotiating a business associate addendum that wasn't necessary at the beginning of the relationship because of the PHE, is especially challenging," Bourque and Compton told *RPP*. "It has been surprisingly difficult for some to negotiate contract terms when they've been working with a business associate counter party for multiple years."

Perhaps adding to these woes are "staffing shortages and adjusting to the constantly shifting regulatory regime when it comes to the use of telehealth more broadly," they said, with licensing, prescribing and reimbursement changes to be handled.

In Bourque and Compton's view, "the most common issue was probably the expedited onboarding of new vendors without the need for a BAA or the typical diligence associated with engaging a new technology provider."

Other Policies Must Again Be Followed

In their comments to *RPP,* they also called attention to the fact that "hospitals providing emergency services under disaster protocols in some cases were given some flexibility under the Privacy Rule for complying" with some requirements—flexibilities that also are over. As a result, hospitals and other providers need to ensure they go back to pre-pandemic policies for the following:

- "Obtaining a patient's agreement to speak with family members or friends involved in the patient's care;
- "Honoring a request to opt out of the facility directory;
- "Distributing a notice of privacy practices;
- "Complying with the patient's right to request privacy restrictions; and
- Complying with the patient's right to request confidential communications."

"Another challenging but necessary operational issue was permitting PHI and patient records to be stored outside of the covered entity with providers working from multiple locations," Bourque and Compton added. "With the importance of keeping infected and healthy patients separated from each other, there simply wasn't time to develop elaborate policies and procedures for off-site operations."

Providers probably can't hope for relief from the HIPAA regulatory issues associated with telehealth, even as some of the telehealth flexibilities have been—or might be—made permanent, either through agency directives or laws passed by Congress.

But they should still pay attention to these developments.

"The telehealth flexibilities that are being extended and made permanent aren't specific to HIPAA and thus do not change HIPAA compliance requirements," the attorneys said. "However, providers [can] take advantage of permanent telehealth flexibilities, such as the ongoing ability to use audio-only platforms for behavioral/mental health care."

If they do so, they still must "consider HIPAA compliance and ensure that services are provided in accordance with HIPAA privacy, security and other requirements on a going-forward basis," Bourque and Compton said. ✧

Endnotes

1. Notice of Expiration of Certain Notifications of Enforcement Discretion Issued in Response to the COVID-19 Nationwide Public Health Emergency, 88 Fed. Reg. 22,380, (April 13, 2023), https://www.federalregister.gov/d/2023-07824.
2. Dianne J. Bourque and Lara D. Compton, "Are You Ready? How to Prepare for the End of OCR's Public Health Emergency HIPAA Enforcement Discretion," Mintz Insights Center, May 1, 2023, https://bit.ly/3suqi4C.

Clearinghouse Inmediata Pays $1.4M In Multistate Agreement After Breach

Puerto Rico-based health care clearinghouse Inmediata Health Care Group LLC agreed to pay $1.4 million to a coalition of 32 states and Puerto Rico and overhaul its data security and breach notification practices in a settlement agreement over a 2019 breach that exposed the electronic protected health information (ePHI) of approximately 1.5 million consumers for almost three years, the states announced.

The settlement—one of two state-based settlements involving PHI announced in October—resolves allegations of the attorneys general that Inmediata violated state consumer protection laws, breach notification laws and HIPAA by failing to implement reasonable data security.

This includes failing to conduct a secure code review at any point prior to the breach and then failing to provide affected consumers with timely and complete information regarding the breach, according to Indiana Attorney General Todd Rokita, who led the coalition.[1]