4. Theresa Defino, "OCR Cautions to Employ 'Good Faith' Efforts, Safeguards, 'Reasonableness' Amid COVID-19," *Report on Patient Privacy* 20, no. 5 (May 2020), https://bit.ly/3cByG5j.
5. HHS, "OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency," news release, April 2, 2020, https://bit.ly/2WjABEI.
6. HHS, "OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency," news release, April 9, 2020, https://bit.ly/2VZhWit.
7. OCR, "HIPAA Privacy and Novel Coronavirus," bulletin, February 2020, https://bit.ly/2KFQ7VS.

Reopening Raises Privacy Risks

continued from page 1

The situation could seem like "a huge mess," in the words of Joseph Lazzarotti, a principal in the Berkeley Heights, New Jersey, office of Jackson Lewis PC, who founded and directs its Privacy, Data and Cybersecurity Practice Group and is also a part of the firm's Employee Benefits Practice Group.

"It's a whole new world…strange times," concurred Reece Hirsch, a partner with Morgan Lewis in San Francisco, who co-leads its privacy and cybersecurity practice. But, he added, "the usual privacy issues have not gone away; they've become more important in situations like this."

"Because it's a national medical emergency crisis, I think there's a natural tendency to move fast and maybe be a little less observant of privacy and security rules," said Hirsch. "And I think OCR has acknowledged that by issuing these statements of enforcement discretion."

On the other hand, "there's also heightened sensitivity to privacy issues in the workplace where you're dealing with this very sensitive information as to whether someone has or hasn't tested positive for COVID-19," said Hirsch. "It cuts both ways. But it's important to remember that the HIPAA rules still apply, and the enforcement discretion that's been articulated is pretty limited in scope and applies very specifically to certain standards during a certain time frame."

Hirsch's recommendation: "The best rule is for covered entities to continue to apply all of the HIPAA standards unless it's just not practical to do so given the circumstances of the crisis."

Match Safeguards to Actual Risks

Since February, OCR has issued FAQs, guidance documents and other information regarding disclosure to first responders; expanded the authority of business associates to disclose information; and enumerated provisions in the privacy rule that may be skipped without fear of enforcement.

But one area it hasn't touched thus far—and where Hirsch said guidance could be useful—is the overlapping roles of employer and CE.

Perhaps the preeminent issue CEs are facing as they try to get back to normal is that of screening both workers and patients for COVID-19 infection or exposure, and what is allowed and what isn't. Further, they need to know if they are creating PHI or not, and how the information must be stored.

An additional consideration is how much information the employer/CE might be able to share with workers about those who may have tested positive.

The Centers for Disease Control and Prevention (CDC) has been the lead agency in issuing guidelines, both for screening patients in health care settings and establishing protocols for when workers who test positive or are suspected of having COVID-19 should return to work.[2]

For example, the CDC points out that "employers are responsible for providing a safe and healthy workplace" and should create a plan to ensure this is the case. Among the activities to consider is the conduct of "daily in-person or virtual health checks (e.g., symptoms and/or temperature screening) of employees before they enter the work site."

Policies and precautions should be equal to the particular risks posed by patients and staff, Lazzarotti added. For example, many health care systems include nursing homes. Because the mortality rate has been so high among those 65 and older, greater precautions are probably required.

Lazzarotti added that any communication that a CE may express must be "consistent with their purpose or their intent," which needs to stem from a clear internal understanding of the screening and reopening plan. Miscommunication might be unintentional and result because "they just haven't thought it through."

Screenings Complicate CE/Employer Role

To begin, it's good to review the fact that "there's a big distinction between health information that a health care provider collects as a HIPAA covered entity and information it collects as an employer," said Hirsch. "Information collected in your capacity as an employer is not subject to HIPAA protections and isn't PHI, so you're operating under a different set of rules."

Hirsch added that "there are areas where the lines cross a little bit. If a health care provider knows that a patient has tested positive for COVID-19, then that has implications for the workforce. But there are HIPAA public health exceptions that would allow disclosure to the provider's employees as necessary to protect health and safety or avoid an imminent threat."

Lazzarotti noted that organizations need to follow state reopening guidelines on screening, which may

vary—and run up against state privacy laws. For example, California has perhaps the strictest laws, with individuals granted a constitutional right of privacy, "but there's also a balancing test that determines whether there is a violation of that."

EEOC Offers Employers Guidance

Organizations could perhaps "argue that these circumstances warrant measures that you might not otherwise take that might offend an employee or a customer's reasonable expectation of privacy," Lazzarotti said.

In early May, EEOC issued guidance on the Americans with Disabilities Act (ADA) and the pandemic.[3] It said, for example, that when an employee calls in sick, the employer legally may "ask such employees if they are experiencing symptoms of the pandemic virus. For COVID-19, these include symptoms such as fever, chills, cough, shortness of breath, or sore throat."

The agency said employers may take a worker's temperature but that doing so is considered part of a medical exam, and results must remain confidential.

In general, the ADA "requires that any mandatory medical test of employees be 'job related and consistent with business necessity.' Applying this standard to the current circumstances of the COVID-19 pandemic, employers may take steps to determine if employees entering the workplace have COVID-19 because an individual with the virus will pose a direct threat to the health of others. Therefore an employer may choose to administer COVID-19 testing to employees before they enter the workplace to determine if they have the virus," EEOC said.

The agency added that employers shall "maintain all information about employee illness as a confidential medical record in compliance with the ADA." A confidential medical file under the ADA is not the same thing as a medical record under HIPAA.

In compliance with the ADA, "a lot of it comes down to whether you, as an employer, are meeting the reasonable privacy expectations of employees," a principle that is reflected in common law as well as under certain state laws, said Lazzarotti.

Lazzarotti said he is getting calls from clients who are "in the weeds," expressing their desire to begin screening for COVID-19 before reopening. "We want to test, we want to use this device, we want to use this app to screen. Is this okay? We're going to do antibody testing. And is that okay?" are among the questions he hears. "I find myself saying, 'Okay, you can talk about that, but let's back up a little bit,'" Lazzarotti added.

Before moving forward, he recommends close examination of the purpose of the screening and then the development of an approach that considers a number of factors. To help guide their thinking, Lazzarotti recommends employers ponder these questions:

- What kind of screening or testing will be used?
- Will workers, patients, visitors and vendors be screened?
- Does the workers' union have to be consulted?
- How will the screening be performed: self-screening, screening by another employee or screening by a device such as a thermal camera kiosk?
- If devices, wearables and/or apps are used, are their capabilities fully understood and are they configured properly?
- Can distancing, sanitization, etc., be accommodated?
- Where will the screening results go? How will the data be shared, if at all?
- How will data be stored and for how long?
- Will third parties be involved, and what arrangements are needed with such vendors?
- Will the program continue past the pandemic?

The answers will "shape the analysis around privacy, practicality and other issues," said Lazzarotti, as employers and CEs put their back-to-work plans together.

Workers Could Use an App

The concept that employee records are to be kept private begs the question about how to conduct screening of employees without individuals nearby learning of the results. As Lazzarotti explained, "If an employee comes in and gets screened, that's a medical examination in the eyes of the ADA. If that employee doesn't pass that screening and if they're on a line of other employees and they turn around and go back out because they can't be admitted, employees on the line are going to have a good sense of the reason why."

One way around this is to keep workers separated, to the extent feasible, said Lazzarotti, and CEs should ensure that tests aren't conducted in a small area. Screenings could be done in a parking lot outside an office or facility. One employer was considering conducting tests near a time clock in a worker break room, an idea Lazzarotti thought might be problematic.

Employees in potentially close quarters are "more likely to learn about the screening results of the employees they supervise," said Lazzarotti, adding that, "because time clocks tend to be inside the facility, the goal of minimizing spread of COVID-19 may be frustrated."

Don't Collect More Info Than Needed

Alternatively, employers are requesting that workers to use an app they can put on their phones that simply asks screening questions, which gives workers something of a pass/fail result they communicate to the employer.

Procedures need to be tailored and adapted to each practice and situation, Lazzarotti said. Those with a lot of employees or seeing a lot of patients "may need a different approach" than performing an individual temperature check, for example. With "a lot of clients, I'm talking through using thermal cameras," he said. But Lazzarotti warned that some of these cameras may have facial recognition capabilities—these should be disabled, in his view.

The use of facial recognition "could pose additional compliance and litigation risks for employers, particularly in states like Illinois," he said.

Hirsch acknowledge there are "questions around record retention requirements," but he added that if the testing is not conducted by licensed providers, "there is not usually an affirmative requirement that those records be maintained."

Still, as an employer, "you want to retain them as necessary to support the employment-related decisions that you're making, but they may not be subject to the same medical record retention requirements that providers are accustomed to," Hirsch said.

'Maximize Patient Privacy'

When it comes to screening patients, do the same principles apply? Perhaps, even if now it may be HIPAA versus the ADA that's the guiding law.

CDC also addressed health care organizations, stating that they should "limit points of entry and manage visitors [and] screen everyone entering the facility for COVID-19 symptoms…regardless of symptoms."

The agency also recommended setting up "separate, well-ventilated triage areas [and placing] patients with suspected or confirmed COVID-19 in private rooms with the door closed and with private bathrooms (as possible)."

Hirsch noted there is a downside to practices that might try to do screening in waiting rooms. This "is something that needs to be handled very carefully, because if other patients get the impression that someone has tested positive or has indicators of COVID-19, they're going to treat that person differently," said Hirsch.

"The layout and the circumstances that a particular office is dealing with are going to vary," Hirsch noted. Regardless, "you should thoughtfully approach those issues in a way to maximize patient privacy. It's different than having your name called out in the waiting room for an appointment. That's a pretty low level of incidental disclosure, which HIPAA permits. But [unintentionally] exposing information to suggest a COVID-19 diagnosis is another matter."

When it comes to both employees and workers, CEs will have to make decisions about how they share information about those who may have COVID-19.

Lazzarotti offered this example: "If a hospital or healthcare provider discovered one of its employees treated at that hospital has COVID-19, you can't turn around and then tell all the other employees, 'Hey, Sally has COVID.' You can say, 'You were exposed. You may have been exposed because one of the employees who works in the same department as you has tested positive.'"

Similarly, a staffing company could disclose to a physician group, hospital or other facility that a worker had COVID-19, he said.

Sharing a Name May Be a 'No-No'

If a patient seems to have COVID-19, HIPAA still applies, said Hirsch, adding that "the minimum necessary rule remains important. That information could be shared to the extent it is necessary to protect the safety of employees who are dealing with that patient. But to share the information more broadly could be inappropriate and a violation of minimum necessary."

Asked whether the provider can reveal the worker or patient's name, Hirsch said there is "no one right answer to that; it's a fact-specific analysis."

An employer may be able to "identify the department or the area of risk, so as to provide the other members of the workforce with enough information to assess whether they have been exposed without stigmatizing a particular employee," he said.

But, added Hirsch, "sometimes it's difficult, because if you're identifying a department and there's only one employee that works in that department, you are effectively pointing the finger" at one person.

Nip Snooping in the Bud

Aside from questions of testing and screening raising new privacy and security questions, the spread of COVID-19 brings with it age-old HIPAA problems, including snooping by workers into patient files and into their coworkers' records.

This is "absolutely going to happen," said Lazzarotti, and CEs need to respond appropriately. A worker might have been checking on a family member or friend, perhaps with the best intentions, but this could mean termination if the CE "has a zero tolerance policy" versus a "graduated disciplinary approach," Lazzarotti said.

He points out that when such a breach does occur, the CE is required to notify the affected patient, per the OCR breach notification regulation, and to include the incident in reports to OCR.

A compliance official who wanted to be proactive about catching snooping could run an audit on all COVID-19 tests and diagnoses to review who accessed patients' records—and determine whether the access was appropriate or not.

CEs should take the opportunity to "remind workforce members that this is not permitted and that there are consequences," said Lazzarotti.

Hirsch agreed. "This is a situation where there's a great possibility for medical records snooping, for inappropriate access to medical records. We see this a lot with public figures, but I think there is going to be a great deal of interest among hospital personnel as to whether another employee has tested positive, or a member of the community or an ex-spouse…there's just going to be a great deal of interest in COVID-19 status."

But he added that "the rules need to be enforced. Even though there's some flexibility that OCR has indicated in various areas, that does not extend to snooping in medical records."

Contact Lazzarotti at joseph.lazzarotti@jacksonlewis.com and Hirsch at reece.hirsch@morganlewis.com. ✧

Endnotes

1. Office for Civil Rights, "HIPAA and COVID-19," HHS, last reviewed June 9, 2020, https://bit.ly/2WJvk9G.
2. "COVID-19 Employer Information for Office Buildings," Centers for Disease Control and Prevention, last reviewed May 27, 2020, https://bit.ly/3eYJAml.
3. "What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws," U.S. Equal Employment Opportunity Commission, updated May 7, 2020, https://bit.ly/2MzhQc1.

PRIVACY BRIEFS

◆ **A divided Indiana Court of Appeals has reinstated a patient's claim that a hospital is vicariously liable for the actions of a medical assistant who accessed the patient's medical records and then shared details with her husband, according to *The Indiana Lawyer*.**[1] The patient, Haley SoderVick, sued Fort Wayne-based Parkview Health System Inc. after Parkview notified her in May 2018 of the disclosure of her protected health information (PHI). SoderVick had gone to an appointment with an obstetrician-gynecologist on Parkview's campus in Wabash in October 2017, and while she was there, medical assistant Alexis Christian accessed her medical records for one minute, the court record shows. "Christian then immediately texted information about SoderVick to Christian's then-husband, Caleb Thomas," Judge John Baker wrote for the majority. "In these texts, Christian disclosed SoderVick's name, the fact that she was a patient, a potential diagnosis, and that she worked as a dispatcher. Christian also texted Thomas that SoderVick was HIV-positive and had had more than fifty sexual partners, although this information was not included in her chart and was ultimately false," Baker wrote. "Christian testified that she had been checking Facebook on her phone during her lunch break earlier that day and had seen that SoderVick had liked a photo of Thomas. Later that afternoon, when Christian was 'inputting chart information and came across all of that information' about SoderVick, she claims she felt 'concerned' and therefore texted her husband asking if and how he knew SoderVick, curious as to whether they might have had a sexual history together." According to the court record, Thomas' sister saw the texts on his phone and notified Parkview, which investigated the potential HIPAA violation, ultimately firing Christian and notifying SoderVick. The case was remanded to the trial court for further proceedings.

◆ **Based in Phoenix, Arizona, District Medical Group (DMG), which includes more than 650 providers in health and medical specialties, said it suffered a breach in February that exposed PHI for more than 10,100 patients.**[2] "On March 11, 2020, we learned that an unauthorized person may have gained access to some DMG employee email accounts through an email phishing incident," the group said in its breach notification statement. The investigation indicates the unauthorized access occurred sometime between Feb. 4 and Feb. 10, the group said. Information that was accessed included patient names, medical record numbers, health insurance information, medical information, and Social Security numbers in some instances, the medical group said, adding that it would offer free credit monitoring for patients whose Social Security numbers were involved.

◆ **In a breach involving a business associate stemming from 2019, Ohio-based Management and Network Services (MNS) has begun notifying[3] more than 30,000 patients that their data may have been compromised.** The company provides administrative support services to post-acute providers and, in connection with these services, may receive information belonging to patients or individuals who were referred by, but did not receive services from, a provider. "On or about August 21, 2019, MNS confirmed that several employee email accounts may have been accessed without authorization at various times between April and July of 2019," the company said in a statement. "Five of the impacted email accounts were believed to contain personal or protected health information." MNS said it took steps to secure the email system and began analyzing the email accounts to determine what information may have been affected,