COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 6. June 11, 2020

# As Covered Entities Inch Toward Normalcy, Thorny Worker, Patient Privacy Issues Arise

By Theresa Defino

Being a health care provider in the midst of a pandemic is complicated enough, between offering telehealth services, perhaps for the first time, and helping workers continue their jobs from home. Such arrangements present new challenges for HIPAA compliance officials, who worry about ensuring these typically less-than-secure remote operations and care methods aren't fodder for increasingly active hackers.

The HHS Office for Civil Rights (OCR) has put in abeyance its enforcement of certain parts of HIPAA, but not the overall foundation ensuring that, absent patient authorization, the use and disclosure of protected health information (PHI) is generally limited to treatment, payment and health care operations.[1]

Now that states have begun to lift stay-at-home orders and practices are reopening for less urgent and more routine and elective services, privacy officials may need to pivot again to help covered entities (CEs) institute precautions, such as screening, to keep both workers and patients at low risk of exposure to COVID-19—while maintaining privacy and adherence to laws, regulations and now new edicts on local levels. Business associates will also have to implement policies and procedures for reopening, and for compliance with HIPAA and their business associate agreements.

The issues are multiplied for hospitals, doctors and other facilities that are in the dual role of employer/provider, increasingly common arrangements as more have vertically integrated with their own health plans. These organizations must comply with different rules that address worker confidentiality, such as the Americans With Disabilities Act (ADA), enforced by the Equal Employment Opportunity Commission (EEOC).

And that's not all: In addition to puzzling out legalities of COVID-19 screening, including when and how data should be kept, HIPAA officials need to be extra alert and act to thwart—and catch—the sometimes irresistible urge among employees to snoop into patient records, no doubt heightened due to the transmissibility of the COVID-19 virus.

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."