HIPAA & The Workplace

BY ELIZABETH J. MCINTURFF, ESQ. AND ISABELLA C. DEMOUGEOT, ESQ., WITH MARIA STRATIENKO

When news broke that professional football players for the Dallas Cowboys and the Houston Texans tested positive for coronavirus, reporters were initially careful to not identify any of the affected players by name. But, as we know, nothing travels as fast as bad news, or in this case, personal health information. "Sources" quickly ran to media outlets to name names, which were then tweeted out to the masses, linking players to diagnoses.

One identified player shot back at the reports, tweeting "HIPAA??"

A SOCIAL MEDIA FIRESTORM ignited regarding the ethics and legality of disclosing another's personal health information. Armchair experts were quick to respond that while the Health Insurance Portability and Accountability Act, otherwise known as "HIPAA", does operate to protect your personal health information from public disclosure, it only applies to specific covered entities. Assuming that none of the players' medical professionals disclosed this information, HIPAA seemingly would not apply.

This discussion is not limited to sports franchises and employers. Rather, this is a critical issue that employers and employees should remain cognizant of as employees return to on-site work. Every business, from mom and pop shops to Fortune 500 companies, should take inventory of their own practices, particularly in the ever-evolving response to COVID-19.

HIPAA may play a significant and material role for many businesses as they reopen their operations. The HIPAA Privacy Rule serves not only as a mechanism for protecting patients' private health information, but also as a means of facilitating the appropriate disclosure of that information to promote public health and safety.

HIPAA may play a significant and material role for many businesses as they reopen their operations.

Responsibilities Under HIPAA – What is it and does it apply to me?

In the case of the identified NFL players, commenters were quick to respond that while HIPAA does operate to protect your personal health information from public disclosure, it only applies to "covered entities" as well as their business associates. But what does that mean for you and your business or employer?

For starters, you should note that HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a *covered entity's workforce*. "Covered entities" include (1) health plans, including individual or group plans that provide or pay the cost of medical care; (2) health care clearinghouses, including third-party intermediaries between health care providers and insurers; and (3) health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services (HHS) has adopted standards. This narrow definition excludes many organizations that may use, collect, access, or disclosure individually identifiable private health information.

Despite this narrow definition of covered entity, individuals and/or businesses alike that perform functions on behalf of a covered entity may also fall into the Rule's scope. These "business associates" and their workforces must comply with the HIPAA Privacy Rule, if and when the activities they perform on behalf of the entity include creating, receiving, maintaining or transmitting protected health information.

These "associates" also include subcontractors that create, receive, maintain or transmit protected health information on behalf of another business associate. With these groups' inclusion, the number of organizations subject to the HIPAA Privacy Rule increases dramatically.

Companies who do not fall into either subgrouping are not subject to the HIPAA Privacy Rule; however, employers with 15 or more employees are subject to the confidentiality requirements imposed by the Americans with Disabilities Act (ADA).

If an employer determines an employee has tested positive for COVID-19 and has potentially exposed others in the workplace, the employer should investigate the potential exposure without disclosing the name or any personally identifiable information of the employee who tested positive. Notably, the ADA's confidentiality requirements do not prohibit the employer from making necessary disclosures to public health authorities and officials.

Notably, entities like biometric identification company CLEAR (known mostly for its presence at airport security) have rolled out products to facilitate employee screening upon phased returns to work. CLEAR is targeting employers to buy this product to use it in their businesses.

However, it remains unclear who retains liability for potential damages if an employee lies during the screening assessment and ultimately infects others. The questions that remain with such products are: a) is the employer liable, b) is CLEAR liable and c) are they both liable? There is the potential for very interesting legislative initiatives and litigation stemming from the rolling-out of such products and services.

Important things for employers to consider

Under the HIPAA Privacy Rule, covered entities and their business associates may share a patient's protected health information (even without express authorization) with public health authorities — including the Centers for Disease Control (CDC) or state and local health departments — for the purpose of preventing or controlling disease or injury. This means organizations subject to the Privacy Rule may report to a health authority that an employee has been exposed to COVID-19, even without that employee's authorization.

If state law permits, a covered entity may also disclose the potential exposure risk to the employees working alongside the employee described as "persons at risk of contracting or spreading" the disease. Finally, a health care provider may share patient information with others as necessary in order to prevent or mitigate a serious imminent threat to public health and safety, so long as that disclosure is consistent with applicable state statutes, regulations and common law.

> The ADA's confidentiality requirements do not prohibit the employer from making necessary disclosures to public health authorities and officials.

While covered entities and business associates enjoy broad latitude in opting to disclose patient information in compliance with public health concerns, these organizations must narrowly tailor the disclosure to provide the "minimum necessary" information to accomplish that purpose.

HHS' guidance on the topic provides that covered entities may rely on public health officials' or authorities' representations that the information they request is the minimum necessary for the purpose, so long as that reliance is **reasonable** under the circumstances.

For example, a covered entity or business associate may rely on the CDC representations that the protected health information requested regarding patients exposed to or suspected or confirmed to have contracted COVID-19 is the minimum necessary amount of information needed.[1] (Emphasis added) In other words, strict compliance with the substance of health authorities' requests for information is unlikely to expose an organization to liability under the Privacy Rule.

Notably, covered entities and business associates may also disclose information to the extent permitted by the individual, who is the subject of the information, as long as that authorization is provided in writing. An individual's personal representatives may also provide the necessary authorization to make such a requested disclosure. The State of Maryland will issue further guidance as we proceed toward conducting business as usual.

Safeguarding Patient Information

It is important to remember the following. Covered entities must implement and retain reasonable safeguards to protect patient information against intentional or unintentional impermissible access, use, or disclosure. These safeguards include (but are not limited to) the guidance and mandates elucidated in the HIPAA Security Rule governing electronic protected health information. Further, as a function of internal security, covered entities should continue to enforce role-based access policies to limit protected health information to the individuals, who need it to perform their duties.

ELIZABETH J. MCINTURFF, ESQ. is a partner, ISABELLA C. DEMOUGEOT, ESQ. is senior litigation associate and MARIA STRATIENKO was a summer law clerk with JDKatz, P.C. – a tax litigation and estate planning law firm in Bethesda, Md. and downtown Washington, D.C.

[1] https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf