HIPAA & COVID-19 – FAQs for Employers Sponsoring Group Health Plans
Last Updated: April 16, 2020

Note: This FAQ will be continuously updated as we continue to gather information related to HIPAA privacy and COVID-19 requirements.

Question 1: What exceptions apply to our plan's use of protected health information (PHI) during a pandemic?

Answer: In general, HIPAA privacy and security restrictions continue to apply as they normally would. Employers sponsoring group health plans should ensure that they only use PHI for purposes of plan administration (e.g., claims adjudication, case management, utilization review, etc.) or other purposes specifically permitted or required by HIPAA, and not for any non-health plan or employment-related purpose without first obtaining written authorization from the individual who is the subject of the PHI.

Keep in mind that employer's may, on behalf of their plans, disclose PHI without first getting written authorization for purposes of public health activities, which may involve disclosures of PHI to a public health authority to ensure public health and safety. These exceptions are discussed in more detail below. (But remember the minimum necessary standard!)

Question 2: What if we have reason to believe an employee has, or has been exposed to, COVID-19? Are we able to share this information with other employees?

Answer: First, consider where this information is coming from. Is it coming from information obtained from the employer's group health plan? Or is it coming directly from the employee? HIPAA would only apply in the first scenario.

<u>Information from the Group Health Plan (PHI)</u>

If the information comes from the employer's health plan records – e.g., on a claims report, then it is PHI and it is subject to protections under HIPAA. Employers, as plan sponsors, may only use or disclose this information for purposes of plan administration or as otherwise permitted or required by law. Sharing such information with other employees would not be permitted. However, as mentioned above, the employer could potentially use or disclose PHI for certain public health activities. For example:

- An employer could disclose PHI to a state public health agency as needed to report all prior and prospective cases of participants exposed to, or suspected or confirmed to have, COVID-19.
- An employer could also disclose PHI if it believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Note that this exception only permits a disclosure to a person (or persons) who are reasonably able to prevent or lessen the threat (e.g., a public health department or a person [or very narrow contingent of persons] in senior management who has the authority to prevent or lessen a threat within the company). This allowance defers to the covered entity's "professional judgment."
- In addition, HIPAA permits disclosures of PHI to persons at risk of contracting or spreading a disease as necessary to prevent or control the spread of the disease or otherwise carry out

public health investigations **if otherwise authorized by applicable law.** So in this case, the employer would need to have some independent legal authority to make this type of disclosure.

Employers should seek the advice of legal counsel before relying on these exceptions for using/disclosing PHI, especially since certain state laws may impose more stringent privacy/confidentiality requirements on employee's medical information than HIPAA does.

Information from an Employee (not PHI)

In the more likely case that an employer learned of an employee's exposure or diagnosis directly from the employee, other confidentiality requirements, such as the Americans with Disabilities Act (ADA), may come into play, so discretion is still advised. Notwithstanding the foregoing, an employer may still have an obligation to let other employees know that they may have been exposed to COVID-19. According to recent CDC guidance, if an employee is confirmed to have COVID-19 (and assuming an employer learns of this diagnosis directly from the employee), the employer should inform other employees of their possible exposure to COVID-19 in the workplace, but should maintain confidentiality as required by the ADA. It can be tricky to balance this obligation with an individual's right to privacy. In light of the current pandemic, an employer's best course of action will be to contact its local public health department to make this disclosure and rely on their guidance for communicating this fact to other employees.

Question 3: Hasn't HHS relaxed some of the normal HIPAA privacy standards in the wake of the COVID-19 pandemic?

Answer: The Secretary of Health and Human Services (HHS) has relaxed some privacy standards for hospitals. But employer-sponsored group health plans must continue to comply with all applicable HIPAA privacy and security requirements.

Question 4: How do we ensure that our health plan's PHI remains protected when our employees responsible for plan administration are all working remotely?

Answer: As part of a plan's HIPAA compliance efforts, it should have what's known as an "emergency mode operations plan" in place. This is similar to a business continuity plan, but specifically addresses how electronic PHI will be protected when normal business operations are disrupted (e.g., due to a global pandemic). Similarly, plans should have safeguards in place for protecting PHI, such as requirements for locked cabinets; secure workstations; and requirements to shred paper copies of PHI. These safeguards would apply to anyone working remotely, so employers should be sure that their workforce understands what their HIPAA obligations are with respect to any PHI handled in their home environments.

Question 5: We're using an IT vendor to assist us with setting up and coordinating work-from-home arrangements. Do we need a Business Associate Agreement with this vendor?

Answer: Business Associates are third parties who assist with plan administration and who require access to PHI in performance of those services. Therefore, if the IT vendor will be working with or providing support for systems that store/maintain/transmit PHI (e.g., shared network folders, filing

systems, email, etc.), then it will be necessary to ensure that a valid Business Associate Agreement is in place with that vendor.

Question 6: We have engaged the services of a telehealth provider to assist with screening/diagnosis of COVID-19 for our employees. What are our HIPAA obligations here, and can we as the employer request test results from this vendor so we can initiate applicable paid leave processes when necessary?

Answer: If the telehealth provider will be providing medical testing/diagnosis services, then the telehealth benefit will be considered a health plan subject to HIPAA and a business associate agreement will be needed with the telehealth provider. Moreover, any information provided by the telehealth provider will be considered PHI and therefore subject to HIPAA privacy and security requirements with respect to uses and disclosures of PHI. These requirements prohibit use of PHI for employment-related purposes (such as administering leave) without written authorization from the individual who is the subject of the PHI.

Question 7: Can I ask an employee directly whether they've been diagnosed with COVID-19?

Answer: Because this information would be coming directly from the employee, HIPAA would not apply, and the employer would need to consult with HR/employment law counsel to ensure that this type of inquiry would not violate other applicable confidentiality laws.

Question 8: Do we need to do anything from a HIPAA security perspective to protect our ePHI during this pandemic?

Answer: During this global pandemic there is a heightened risk of cybersecurity incidents, including hacking and phishing attempts. Plan sponsors are advised to revisit their HIPAA Security Risk Analyses in light of these increased threats to ensure that their security controls are sufficient to protect against any risks. It may also be advisable to provide additional or supplemental security awareness training to employees.