BLANKROME

Cybersecurity & Data Privacy

MARCH 2020 • NO. 2

Coronavirus Alert: Ensuring Privacy in a Time of Crisis

In what feels like the blink of an eye, the coronavirus ("COVID-19") has reached the shores of the United States and spread across the country in an unprecedented fashion. On March 13, 2020, President Trump officially declared a national emergency over the coronavirus pandemic. As the crisis expands further, employers are becoming increasingly concerned with ensuring the health and safety of their employees. Importantly, however, while the coronavirus epidemic presents significant issues regarding the wellbeing of employees and the public at large, companies must keep in mind that even during the current crisis, they must still adhere to the range of differing privacy laws and obligations that govern the collection, use, and disclosure of personal information.

THE TENSION BETWEEN PERSONAL PRIVACY & PUBLIC SAFETY IN THE TIME OF A PUBLIC HEALTH CRISIS

Currently, in their attempt to ensure the health and wellbeing of their workforces, employers are grappling with the significant tension that exists between public health and personal privacy. As the coronavirus continues to increase exponentially across the country, employers are now moving to unprecedented measures, such as checking employees' temperatures and making inquiries as to the health status of workers' household family members, as part of their coronavirus response and containment efforts. In addition, many employers are also facing tough decisions regarding whether to disclose that a colleague has tested positive for the virus and, if so, how much information should be shared with other workers. The current situation places every employer in unchartered territory.

These issues are significantly magnified because of the new wave of privacy laws that have recently been enacted across the country—most notably, the California Consumer Privacy Act of 2018 ("CCPA")—which place significant limitations and requirements on the collection and use of personal information. At the same time, other laws which contain privacy requirements, such as the Health Insurance Portability and Accountability Act ("HIPAA") and American With Disabilities Act ("ADA"), provide an additional layer of compliance obligations when it comes to collecting, using, and sharing employees' personal and health information.

Combined, and even in the face of relaxed rules while under a government pandemic declaration, employers must proceed with great caution and care when seeking to collect, use, and share coronavirus-related personal information not only to strike the right balance between personal privacy and protecting the health of their

workforces as a whole, but also to ensure that employers stay in line with their privacy-related legal obligations, which provide for significant penalties for non-compliance.

COMPLIANCE STEPS

To strike the proper balance between ensuring personal privacy and protecting the health of the public, while at the same time maintaining compliance with today's patchwork of privacy laws, employers should consider the following best practices:

Proportionality/Data Minimization: As a starting point, employers should adhere to the principles of proportionality and data minimization when dealing with issues regarding the collection and use of coronavirus-related personal information. If an employer seeks personal information from employees, only that information which is fundamental to achieving the goal of effectively managing risk and safeguarding the health and wellbeing of its workforce should be collected. Similarly, if an employer finds it necessary to disclose information about an employee who tested positive for the coronavirus, it is permissible to inform other employees of their possible exposure to the coronavirus in the workplace, but such disclosures should be as nonspecific as possible—leaving out any details that could potentially identify the sick individual—while still providing sufficient details that will allow other employees to make informed decisions about the appropriate actions to take. In addition, if an employer is informed of a confirmed case of COVID-19, it should work with law enforcement and public health officials to provide the appropriate notice of positive coronavirus test results as well.

Facts, Not Speculation: Also, it is important that in making any type of disclosure or notice, employers avoid speculating as to whether any individual has tested positive for the virus. Rather, employers should stick to facts and disclose, or report only ***confirmed*** positive COVID-19 test results.

Privacy Notices/Disclosures: In addition, many new privacy laws, including the CCPA, require companies to provide a "notice at collection" which mandates—in addition to maintaining a general privacy policy—just-in-time notices to individuals at or before the time any personal information is collected (and bars the collection of data in the absence of such notices). As such, employers should determine whether they are subject to any such requirements and, if so, should ensure that just-in-time notices are issued when any coronavirus-related information or data is collected.

HIPAA Disclosures: Employers that sponsor health plans may receive health information about employees through their plans, which is covered by HIPAA as protected health information ("PHI"). Recently, the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") issued useful guidance regarding disclosures in the context of the current coronavirus public health crisis. Of note, the guidance provides that it is permissible to make disclosures of PHI about individuals suspected of having contracted the coronavirus to public health authorities that are authorized by law to receive such information for the purpose of preventing or controlling the spread of disease. In addition, covered health plans may share protected PHI with anyone "as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public," consistent with applicable law.

Data Security Measures: Employers also need to ensure that they continue to maintain effective cybersecurity safeguards during the ongoing coronavirus outbreak, especially as cyber criminals have stepped up the frequency of their cyber-attack campaigns to take advantage of the public's significant panic and fear regarding the current health crisis. In particular, as there has been a noteworthy spike in phishing attacks disguised as providing coronavirus-related health materials, companies should consider educating employees on how to spot attempted phishing attacks and best practices to follow. For additional information on how to guard against the significant risk of coronavirus-themed phishing attacks, please view our Coronavirus ("COVID-19") Task Force article on this topic here. Finally, to further aid in minimizing data security risks, employers should also consider implementing protocols for the manner in which it will collect, retain, secure, and delete personal information that is collected as part of its coronavirus response, especially as it relates to sensitive health information.

THE FINAL WORD

As the coronavirus continues to spread, employers must take appropriate action to safeguard the health and wellbeing of their employees. Importantly, employers cannot achieve this objective without having adequate

information to make informed decisions about the appropriate course of action to take as part of their coronavirus response efforts. However, in doing so, employers must also balance public health and safety with personal privacy considerations. Equally as important, employers must also ensure that they maintain compliance with today's complex web of privacy laws and regulations while protecting the health and safety of their workforces.

If you are considering collecting, using, or sharing any personal information of employees or others as part of your coronavirus response efforts, you should speak with experienced legal counsel to ensure that your organization has in place the proper policies and practices that will ensure compliance with your privacy legal obligations.

As part of Blank Rome's Coronavirus ("COVID-19") Task Force, the Firm's cybersecurity/privacy and employment professionals can assist with providing key counseling and guidance with respect to any privacy issues or concerns relating to the collection, use, or disclosure of personal information, as well as the necessary policies, procedures, and protocols that employers must have in place to comply with applicable privacy laws when utilizing personal information to take appropriate action while the coronavirus crisis persists.

For additional information, please contact:

Jennifer J. Daniels | Cybersecurity & Data Privacy
412.932.2754 | daniels@blankrome.com

Brooke T. Iley | Labor & Employment
202.772.5816 | iley@blankrome.com

David J. Oberly | Cybersecurity & Data Privacy, Privacy Class Action Defense
513.362.8711 | doberly@blankrome.com