The California Consumer Privacy Act (CCPA) had only been in effect for a short time before the COVID-19 pandemic struck, raising a host of new privacy challenges for employers in the midst of trying to comply with an entirely new set of challenges and laws. As California businesses begin to reopen, these concerns have only increased – and will only amplify once the enforcement date of the CCPA kicks in on July 1, 2020. What do employers need to know about complying with California’s new privacy law during the COVID-19 era?

**Does The CCPA Apply To Your Business?**

At the outset, it is important to determine whether the CCPA applies to your business. Check out our blog posts on California’s Groundbreaking Privacy Law and whether it applies to franchisees, subsidiaries, and affiliates to determine if your business must comply with the law’s requirements.

**Health Screenings And Temperature Checks**

As businesses begin to reopen, most county public health orders require employers to implement protocols to limit the transmission of COVID-19 in the workplace. Many of these orders require that essential and reopened businesses put in place measures for employee and customer health screenings and/or temperature checks. Before doing so, you should prepare and issue privacy notices that are compliant with the CCPA.
What Is Required Under The CCPA?

As of January 1, 2020, the CCPA requires, among other things, that a covered employer provide a notice at or before the collection of the personal information of employees, job applicants, or independent contractors that is collected in the course of employing, recruiting, or contracting with them. A covered business must also provide a notice to all other consumers at or before the collection of their personal information. As a reminder, the CCPA broadly defines personal information as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

The notice must identify all the categories of personal information and list the business purposes for which each category of personal information will be used. Businesses are prohibited from using the personal information collected for any other reason that is not specifically listed on the notice. Thus, it will be necessary to develop a notice for employees (a category that includes for this purpose job applicants and independent contractors) and a separate notice for non-employee consumers to properly identify the personal information collected about each group.

How Does COVID-19 Impact Employers’ CCPA Obligations?

Due to the requirements of many local public health orders, you may find your business collecting additional health information, travel information, biometric data, geolocation data, or even information about employees’ family members with COVID-19 symptoms. This information undoubtedly meets the definition of personal information under the CCPA.

At or before collection, you are obligated to provide employees with a notice if no prior notice covering the information has already been provided. Additionally, you will also need to list the COVID-19 related business purposes that the collected information will be used for, such as reducing the risk of COVID-19 in the workplace and to permit contact tracing.

This notice requirement applies only if information is retained beyond the point at which your business may check temperatures or symptoms. In the non-employee consumer context, if you simply check a customer’s or other guest’s temperature before letting them into a store, office, or facility, and the information is not actually retained in a manner that can be linked to the individual, then the CCPA obligation is not triggered. Conversely, in the employee context, even if no information such as a particular employee’s temperature is immediately recorded, the results of the screening will more than likely be retained.

For example, if an employee is sent home for having a fever, it seems likely that their manager or the human resources department will retain a record of the employee being sent home and the reason for which that occurred – especially to track their attendance and to facilitate a follow-up to
ensure they do not return to the workplace with symptoms. Thus, even if you do not retain a log with employee names and corresponding temperatures, some information is almost certainly being collected and retained. Thus, the CCPA notice obligation would be triggered with respect to employees entering the workplace.

If your business has not already provided this CCPA notice, now is the perfect time to prepare a notice that includes the general information collected about consumers, as well as the information that you collect from health screenings and temperature checks. If you have already provided the more comprehensive notice to your consumers or employees – which ideally would have been provided on or before January 1, 2020 – you should supplement the notice to include personal information that will be collected from health screenings and/or temperature checks.

It is important that you provide this notice at or before the collection of health information. For example, if you require employees to perform at-home screening and report their results via an online survey, you may provide the notice on the website page where employees will input their results. For in-person screenings, you should give the notice before the employee or customer provides answers to health screening questions or has their temperature taken.

Must Consumers Sign The Privacy Notice?

Whether collecting information from at-home employee self-screenings or taking temperatures at the door of the workplace, it is critical that you comply with the notice requirement under the CCPA. Failure to do so could result in civil penalties from $2,500 for a non-intentional violation to $7,500 for an intentional violation.

A common question is whether employees and customers must sign the CCPA notices or otherwise acknowledge receipt. While the CCPA does not require consent to collect health and temperature information, we recommend requiring signatures as a standard practice. This will serve as an acknowledgement that the consumer received the notice, and was made aware of the personal information collected and for what business purposes the information would be used.

Storing Health Information

Unless required by a local order, we recommend that you not record the results for all health screenings and/or temperature checks. If you collect or distribute any medical or health information, there is an increased risk of privacy-related claims concerning the storage of the information. You may choose to only record whether an employee “passed” or “failed” the health screening and/or temperature check in order to limit the amount of personal information stored.
Regardless of whether you choose to collect and record personal information, you must implement reasonable security measures, both physical and electronic, to protect against the disclosure or misuse of personal information. When storing health information of employees, you should maintain this information in a confidential medical file separate from the employee’s personnel file. You should also limit access to the employee’s health information to only those individuals who need to access it. You should store confidential medical files in a locked cabinet and, if stored electronically, encrypt the data. You should not retain consumers’ health information longer than is necessary to serve its purpose.

The CCPA provides consumers with a private right of action for unauthorized access and disclosure of their personal information. We have already seen several class action lawsuits alleging a failure to provide reasonable security measures that resulted in a data breach. To minimize the risk of litigation, you should designate an individual who will be responsible for privacy compliance and update existing privacy policies to match industry standards.

**Disclosing Health Information**

In the case of a positive COVID-19 test, you should have policies and procedures in place to identify all individuals who worked in close proximity of the individual. After you engage in contact tracing, it will be necessary to notify all employees who worked near the infected employee. You can use this Model Announcement to Employees About a Positive COVID-19 Test. In accordance with the CDC’s guidance and the Americans with Disabilities Act (ADA), you should not reveal the identity of the employee or a coronavirus diagnosis, unless the employee has signed an Authorization to Disclose their COVID-19 Diagnosis.

**Enforcement Of The CCPA During COVID-19**

The California Office of the Attorney General issued an alert on April 20 reminding consumers of their privacy rights under the CCPA during COVID-19. Despite the ongoing pandemic, the Office of the Attorney General indicated that it will still begin enforcement of the CCPA on July 1, 2020.

**Takeaways**

As businesses begin to reopen and return to the workplace, you should take immediate action to evaluate existing privacy practices and implement the requirements of the CCPA. This includes providing notices to consumers about what information will be collected during health screenings and/or temperature checks, and putting in place reasonable security measures to safeguard personal information.
To summarize, we have created a checklist detailing the steps that you should take prior to conducting health screenings and/or temperature checks to ensure your business is CCPA complaint:

- Implement reasonable security measures, physically and electronically, for all stored data. This includes ensuring physical files are stored in locked cabinets and that electronically stored data is encrypted.

- Update your privacy policy to match industry standards.

- Determine whether you will be storing health screening and/or temperature check data from non-employee consumers (customers and visitors). If so, provide a CCPA complaint notice to non-employee consumers that includes the categories of personal information that you will collect from the health screening and/or temperature check, and the business purposes for which each category of personal information will be used.

- If you have already provided the more comprehensive notice (which ideally would have been provided on or before January 1, 2020), you should supplement this notice with a notice that includes the categories of personal information that you will collect from the health screening and/or temperature check, and the business purposes for which each category of personal information will be used.

- If your business has not already provided a notice to employees, you should issue a notice to employees that contains general categories of information collected about consumers, as well as the information that you collect from health screenings and/or temperature checks, and the business purposes for which each category of personal information is used.

Store employee health information gathered from the health screenings and/or temperature checks in a confidential medical file and limit access to those individuals who need access.

Fisher Phillips will continue to monitor the rapidly developing COVID-19 situation and provide updates as appropriate. Make sure you are subscribed to Fisher Phillips’ Alert System to get the most up-to-date information. For further information about compliance with the CCPA, contact your Fisher Phillips attorney or a member of the Fisher Phillips’ Data Security and Workplace Privacy Group. You can also review our FP BEYOND THE CURVE: Post-Pandemic Back-To-Business FAQs For Employers and our FP Resource Center For Employers.

This Legal Alert provides an overview of a specific developing situation. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.