Blogs
March 19, 2020
CCPA & COVID-19: A Practical Guide to Addressing Privacy and Data Security Implications of the Coronavirus

COVID-19 arrives just as the first omnibus privacy statute in the United States, the CCPA became effective. Since its January 1 effective date, we continue to wait for finalization of the CCPA regulations and enforcement that was slated for July 1. In a pandemic environment, companies, employers, and public institutions are grappling, outside the HIPAA context, with unique privacy, data security, and cybersecurity implications of their responses to the coronavirus. From a compliance perspective, businesses are considering under what circumstances they can disclose consumer or employee health conditions or geolocation information in the service of greater public health. Other companies —and governmental institutions at every level—are confronting the very real, and often opportunistic threats to data security posed by aggressive thieves who use crises as cover to commit an assortment of cybercrimes. Privacy and security requirements vary by jurisdiction, so businesses should be mindful of potentially divergent and overlapping approaches and responsibilities as the situation continues to evolve. We offer a few updates and practical tips for best practices to promote compliance with privacy and data security requirements. **Guidance for Collecting and Sharing Health Information for Businesses That Are Not "Covered Entities" Under HIPAA** As they respond to the coronavirus, companies need to address the legal implications of collecting and/or sharing health information regarding their employees and customers outside the HIPAA context. Employers are dealing with how to disclose an employee's coronavirus diagnosis to their workforce and public health authorities. Restaurants are considering whether they can assess customers presenting coronavirus symptoms before letting them into their establishments. Delayed supply chains require businesses to increase their communications with customers from remote operations. In the United States, the California Consumer Privacy Act (CCPA) governs the collection, disclosure, and sale of personal information--including health information such as medical symptoms and diagnoses. Best practices under the CCPA center on notice and security. Unlike the EU, the CCPA does not require a legal basis to process information. Under the CCPA, consent is required in limited circumstances (e.g. parental consent for children's data, adult opt-in, and authorized agents). The CCPA currently provides a qualified employer exemption. *See* Cal. Civ. Code §1798.145(h). However, employers are still subject to notice (1798.100(b)) and data security (1798.150)) requirements. Employers may reasonably use personal medical and health information to make internal decisions regarding remote work plans and business contingencies. However, the employer exemption applies to personal information of a job applicant or employee solely within the context of their employment. Disclosing personal information, including medical or health information, of employees, outside the employment context, is subject to notice and opt-out requirements. *See* 1798.100(b). Employers and companies should do the following before collecting or sharing health information:

- **Update personnel and consumer-facing privacy policies to capture the category of personal information collected and the purposes for the same.** If a company is considering collecting health information, including temperatures, symptoms, or diagnoses, it should ensure that employees and customers have notice at the time of collection. Likewise, if a company is considering sharing such information with its workforce, customers, or public health authorities, it should list those disclosures as a potential purpose in its policies. *See* 1798.100(b); 11 C.C.R. § 999.308(c).
- **Consider offering an opt-in for collection and disclosure of sensitive medical information.** Medical information, including medical history, treatment, and diagnosis, is considered presumptively sensitive under California law, increasing the compliance responsibilities of anyone collecting that data. *See* 999.323(b)(3)(a); 1798.81.5(d)(1)(A)(iv). Companies may offer individuals the opportunity to opt-in to the disclosure of such information. *See* 999.316.
- **Do not disclose the identity of an employee with a coronavirus diagnosis.** Employers should treat their employees' medical information with strict confidentiality. In accordance with the CDC's Interim Guidance for Business and Employers and the Americans with Disabilities Act (ADA), an employer

should not disclose the identity of an employee or a coronavirus diagnosis unless disclosure to safety and first aid personnel is required for emergency treatment. *See* 42 U.S.C. §§12112(d)(3)(B), (4)(C).

Guidance for the collection and sharing of geolocation data As the government and public struggle to contain the spread of COVID-19, many, including government officials, are calling for the use of AI and machine learning technology to track infected individuals and discern who else may be impacted. Technology companies are considering projects that use de-identified and aggregate location data to map the spread of the coronavirus, or to determine if individuals are practicing sufficient social distancing. Businesses may face questions regarding whether they can collect geolocation information for such data aggregation efforts and if they can share the information in response to requests from data aggregators and still comply with applicable privacy laws. We suggest some guidelines and considerations for businesses collecting and sharing geolocation data that will help them navigate these unique questions. Businesses that collect geolocation data on employees and/or customers in high risk areas through mobile applications or other devices should follow FTC guidelines and requirements under the CCPA, if applicable. Geolocation data is considered "sensitive data" and subject to stronger data protection requirements when it can reasonably be linked to an individual. The CPRA, a new California ballot initiative to amend the CCPA, defines "precise geolocation data" as data that can locate a consumer within a geographic area the size of a circle with a radius of 1,850 feet. Given the sensitivity of this data, businesses should do the following prior to collection and/or sharing:

- **Update their privacy policies to give notice of collection of geolocation data and how it will be used.** Ensure that all privacy policies which apply to the consumer/employee adequately disclose that the company will collect geolocation data and the purposes of the collection (to maintain a safe and healthy workplace; to share with public health authorities, to share with data aggregators, etc.). Giving adequate notice prevents the collection and/or disclosure of geolocation data from being considered "deceptive" by the Federal Trade Commission ("FTC"), and comports with the CCPA's requirement to provide notice of the purposes for collection of "personal information," which includes geolocation data. *See* 999.308(c).
- **Obtain opt-in consent with a "just in time" notice to consumers.** If employees are using company property, opt-in consent is not usually required for collection of geolocation data, so long as adequate advanced notice of collection and the purposes for collection have been provided. With respect to consumers, however, the collection of geolocation data is subject to additional requirements. Pursuant to FTC guidelines, companies are required to provide a "just in time" notice and obtain opt-in consent prior to collecting geolocation data of consumers, even if location is inferred from a wi-fi network. The most recent draft of the CCPA regulations also requires "just-in-time" notice prior to collecting location data, which should contain a link to the full notice in the company's privacy policy (999.305(a)(4)). The regulations give as an example the use of a pop-up window that contains the required notice when the consumer opens the application.

Immediately prior to the initial collection of or transmission of geolocation information, on a separate screen from any final "end user license agreement," "privacy policy," "terms of use page" or similar document, the following should be disclosed clearly and prominently:

- The application collects, transmits, or allows the transmission of geolocation information;
- How geolocation information may be used;
- Why the application is accessing geolocation information; and
- The identities or specific categories of third parties that receive geolocation information directly or indirectly from the application (i.e. the information may be shared with public health authorities)

The "just-in-time" notice should allow the user to affirmatively consent to the collection of geolocation data, such as with a check box, and should link to the full notice in the company's privacy policy in accordance with CCPA regulations.

- **Only collect or infer geolocation information after confirming that:**
  - the consumer provided affirmative express consent;
  - the consumer has not expressed that they do not consent to or revoked consent to collection; and
  - the consumer has not expressed that the consent to collection of location information is limited to a level of accuracy that is less precise than the location information that is to be collected or inferred.

For Global Operations, Considerations in Light of EU Approach For businesses with global operations, data privacy considerations don't stop at the border, and they will need to meld their global privacy program with CCPA compliant practices as part of a top-line privacy approach. The EU's General Data Protection Regulation (GDPR) applies to all data processing activities of companies doing business in the EU or that process information of EU residents. Companies subject to GDPR should ensure that their data processing activities in connection with COVID-19 (i) comport with exemptions in the GDPR, (ii) follow guidelines issued by the applicable data protection authorities, and (iii) account for principles of proportionality and minimization. The GDPR contemplates the necessity of data processing in the interest of public health, stating in its recitals the need for lawful processing activities that serve "the public interest and the vital interests of the data subject ... including for monitoring epidemics and their spread." Article 9(2)(i) exempts the processing of data related to health, which is otherwise considered sensitive data prohibited from processing, when "protecting against serious cross-border threats to health...on the basis of Union or Member State law." On March 16, 2020, the European Data Protection Board issued a statement confirming that the GDPR provides the legal grounds to enable employers to process data in the context of epidemics such as COVID-19 without consent of the employee, while advising that local laws and the ePrivacy Directive will cover location data on mobile applications and may still require consent under those separate laws. ***Italy and France - no autonomous systematic data collection initiatives*** Given that the exemption in Article 9 for processing of health data is tied to Union or Member State law, Companies should track and follow the guidance of data protection authorities in the applicable jurisdictions. An overarching theme among Member States is that employers should focus more on measures that facilitate self-reporting by employees, rather than implementing comprehensive data collection programs in response to the coronavirus. Businesses should review the guidance issued by data protection authorities in Italy and France, described below, but should in addition consult guidance in any relevant jurisdictions. The IAPP has published a chart of guidance from data protection authorities in various jurisdictions to aid companies' review. Companies doing business in Italy or France should not conduct autonomous systematic collections of health data from employees located in those jurisdictions, including asking for information regarding potential symptoms, required temperature-taking, or requests for medical information. Italy's data protection authority, the Garante, has issued guidance that collection of health data related to COVID-19 must be left to the public health authorities. The French data protection authority CNIL, in its guidance, gives examples of unlawful processing that include collecting daily temperature readings from employees and visitors, and collecting medical files from all employees. Instead, businesses should focus on helping employees self-report contact with the coronavirus. Employees in Italy and France have a duty to protect the health and safety of others in their work environment, which includes an obligation to inform employers of any suspected contact with or symptoms of the coronavirus. The CNIL's guidance promotes training employees to self-report this information and encourages employers to establish communication channels to receive information. The CNIL regards as lawful processing an employer's recording of the date and identity of the reporting employee, along with the business's response to the report. ***Travel Questionnaires*** Businesses seeking to use travel questionnaires to determine if employees or visitors have recently visited a high-risk area for COVID-19 may generally do so under the GDPR, except for businesses in Italy, due to the Garante's expectation that the collection of such data be done by public health authorities. The use of travel questionnaires has been interpreted in EU states to be proportionate to the legitimate interests of the business under Article 6(1)(f) to maintain health and safety in the workplace. Before using travel questionnaires, however, companies should consult any guidance of the local data protection authorities to ensure that the travel data collected is deemed reasonable and proportionate there. ***Data Minimization and Proportionality*** Only the minimum necessary data should be collected and processing activities should be proportionate to the company's legitimate interests in

responding to COVID-19. For example, a company's interest in maintaining a safe and healthy workplace will generally not require the employer to share the identity of an employee that has reported symptoms of COVID-19 with other employees. Rather, the employer should notify the proper public health authorities of employees that tested positive and follow the advice of the authorities regarding disclosure to others. **Securing data against cybersecurity threats** The coronavirus creates crisis conditions and lack of focus that provides prime ground for data thieves to operate unnoticed. Healthcare companies and public institutions are especially vulnerable because their attention is fixed firmly elsewhere. For example, just a few days ago, on March 14, the U.S. Department of Health and Human Services reported a cybersecurity attack aimed at its systems. Phishing email scams containing dangerous malware often pose as innocent coronavirus updates or government warnings, while other emails may pose as an employer with details regarding a company purchase of health supplies or a remote-work plan, directing employees to disclose sensitive personal or financial information by way of response. In light of these cybersecurity attacks, businesses should remain vigilant to potential vulnerabilities, step up their protective measures to harden their data borders, and document their efforts to ensure maintenance of a good evidentiary history of their actions and efforts. Companies should consider the following measures:

- **Identify where sensitive data is stored and any technical controls regarding information security.** Sensitive information (e.g. SSNs, credit card info) may be especially at risk to a data breach. If a company does not know where its sensitive information is stored, consider scheduling a meeting with the information security team soon.
- **Ensure that contact information for all employees to verify identity is updated and that the business has access to such information.** Updating employee contact information will ease the shift to remote operations and be essential for an emergency response.
- **Consult the business's risk assessment (e.g. NIST or ISO) and identify any mitigation measures for high-risk processing.** Companies should reacquaint necessary employees with their data assessment to ensure it is up-to-date regarding potential vulnerabilities and response plans.
- **Review the business's remediation plan.** Companies should ensure there is a way to reliably reach all essential personnel in the event of a data breach. Reduced staff may create additional vulnerabilities, so companies should verify that they have the necessary monitoring staff and technical controls for a remote work response to critical incidents.

Takeaways The rapid onset of COVID-19 has forced businesses to make fast decisions that require balancing their interest in protecting the health and safety of others with data privacy and security concerns. To recap, our recommendations to businesses are:

1. Update all internal and consumer facing privacy policies to provide notice of the types of data collected and purposes for which it will be used.
2. Provide an opt-in mechanism for sensitive data such as medical data and geolocation data.
3. Evaluate data processing activities in the EU and comply with applicable DPA and local Member State guidelines for processing data, especially location data.
4. Collect and use data only in accordance with the notice given in your privacy policy and respect data minimization and proportionality principles.
5. Secure the business's systems and its data against cyber threats with technical controls, risk assessments, and a remediation plan.

Authors

Explore more in

Privacy & Security