FAQs – Cybersecurity and Privacy

1. Question: The law requires certain businesses to maintain “reasonable security procedures.” What is considered “reasonable” in light of the coronavirus (COVID-19) outbreak?

“Reasonable security procedure” is undefined. What is “reasonable” depends on the size of each business and the nature of the data each collects. As a result, many organizations rely on guidelines and frameworks when making decisions (e.g., NIST Cybersecurity Framework, Top 20 CIS Controls, etc.). However, as COVID-19 continues to spread and businesses worldwide are forced to shift abruptly to a work-at-home workforce, the question arises as to whether the standard for “reasonable security” changes. It likely does. For an in-depth discussion, see our publication, [*COVID-19 Warrants Modified Cybersecurity for Work-at-Home*](https://www.consumerfinancialserviceslawmonitor.com/2020/03/covid-19-warrants-modified-cybersecurity-for-work-at-home/)*.*

1. Question: With all that is going on, why should businesses prioritize cybersecurity?

While protecting the health of employees and clients should be every organization’s top priority, businesses would be naïve to ignore the cyber risks presented by COVID-19, which has forced a majority of businesses to shift to remote work. Hackers, looking to capitalize on fragmented operations and inherent employee vulnerabilities that exist, even in absence of crisis and panic, are leveraging COVID-19 to carry out attacks. For an in-depth discussion and a few basic precautions every business should take, see our publications, [*Cybersecurity Tips to Prevent Your Business from Becoming COVID-19’s Virtual Victim*](https://www.troutman.com/images/content/2/2/v2/224303/Cybersecurity-Tips-to-Prevent-Your-Business-from-Becoming-COVID.pdf) and [*Beware: Phishing Scams Prey on Coronavirus Fears*](https://www.pepperlaw.com/publications/beware-phishing-scams-prey-on-coronavirus-fears-2020-03-18/).

1. Question: What privacy considerations should be at the forefront of each organization’s planning as they tackle the operational effects of COVID-19?

As COVID-19 continues to spread, businesses face pressure to make swift decisions that impact not only business operations, but also the privacy and security of employees’ personal information. In times like these, the Fair Information Practice Principles (FIPPs), which provides the foundation for many U.S. state and federal privacy laws (*e.g.*, the California Consumer Privacy Act [CCPA] and the Heath Insurance Portability and Accountability Act [HIPAA]), should be every organization’s guiding light. For an in-depth discussion, see our publication, [*Notice to Employers: Remember Privacy Basics When Addressing COVID-19*](https://www.troutman.com/images/content/2/2/v2/224329/Notice-to-Employers-Remember-Privacy-Basics-When-Addressing-COV.pdf).

1. Question: Our operations rely heavily on certain critical service providers and suppliers. While we have internally prepared to tackle the effects of COVID-19, we are concerned about our vendors. What can we do to address the impact of COVID-19 downstream?

All business should reach out to vendors to discuss the disruptions caused by, and the changes needed to address, COVID-19. At a minimum, businesses should be requesting assurances that there is a plan in place to address the impact of the outbreak in stages (*e.g.*, 30-60-90-120-180 days), so that Vendor’s efforts can be appropriately scaled, consistent with the effects of a particular stage of the outbreak, which includes an assessment of how quickly measures could be adopted and how long operations could be sustained under different stages of the outbreak. For a template designed to assist in drafting a custom letter to critical service providers and suppliers, see [here](http://covid19.troutman.com/resources/Template_-_Request_for_Assurance_from_Critical_Vendors_of_Operational_Preparedness_to_Address_COVID-19.pdf).

1. Question: What is the latest update on California Consumer Privacy Act (CCPA) enforcement?

Pursuant to Cal. Civ. Code section 1798.185(c), the California Attorney General (AG) may not bring an enforcement action under the CCPA until six months after the publication of the final regulations or July 1, 2020, whichever comes first. Given the regulations have not been finalized, enforcement will likely begin in July. Although many organizations and trade associations are pushing the AG to delay enforcement due to the COVID-19 outbreak, there has been no indication from the AG that enforcement will be delayed. For an in-depth discussion relating to CCPA enforcement, see our publication, [*CCPA Enforcement Alert: Businesses Must Not Ignore CCPA Requirements During COVID-19 Pandemic*](https://www.pepperlaw.com/publications/ccpa-enforcement-alert-businesses-must-not-ignore-ccpa-requirements-during-covid-19-pandemic-2020-03-27/).

For companies who have already made effort to comply with CCPA, it will be critical to determine what adjustments, if any, need to be made in light of COVID-19. For example, businesses should evaluate their service providers’ capabilities to assist in honoring consumer requests (see FAQ No. 4 above). Similarly, businesses may also want to evaluate their own ability to comply with consumer requests within the time required or consider whether extensions need to be requested.

For businesses who have not considered the CCPA, it is still not too late. Refer to our infographic published by the International Association of Privacy Professionals (IAPP), [*Is Your Business In Need of a CCPA Intervention?,*](https://iapp.org/resources/article/infographic-is-your-business-in-need-of-a-ccpa-intervention/) to get the CCPA conversation started within your organization.

1. Question: What are the implications of COVID-19 on HIPAA?

The U.S Department of Health and Human Services (HHS) has provided limited relief from enforcement of certain provisions of HIPAA during the COVID-19 nationwide public health emergency. On March 15, HHS issued a waiver of sanctions for noncompliance with the patient’s right to request privacy restrictions and confidential communications and the requirements to obtain a patient's consent to speak with family members or friends involved in the patient’s care, honor a request to opt out of the facility directory, and distribute a notice of privacy practices. On March 17, the Office for Civil Rights (OCR) at HHS announced it would exercise its enforcement discretion and waive potential penalties for HIPAA Privacy Rule violations related to the use of certain remote communication technologies to provide telehealth services. On April 2, the OCR announced that, effective immediately, it would exercise its enforcement discretion over certain provisions of the HIPAA Privacy Rule by not imposing penalties on health care providers or their business associates that use and disclose protected health information (PHI) in “good faith” for public health and health oversight activities. For an in-depth discussion, see our publications, [*HHS Waives HIPAA Sanctions to Facilitate Suppression of Coronavirus*](https://www.pepperlaw.com/publications/hhs-waives-hipaa-sanctions-to-facilitate-suppression-of-coronavirus-2020-03-19/) and [*HHS to Exercise Enforcement Discretion Over HIPAA Privacy Rule for PHI Disclosures by Business Associates*](https://www.pepperlaw.com/publications/hhs-to-exercise-enforcement-discretion-over-hipaa-privacy-rule-for-phi-disclosures-by-business-associates-2020-04-03/).