HITRUST

The California Consumer Privacy Act *FAQs*

FAQs are specific to this webinar. Visit our General FAQs here.

Q: The term 'resident' as defined in Section 17014 of Title 18 of the California Code of Regulations includes 1) every individual who is in the state for other than a temporary or transitory purpose, and 2) every individual who is domiciled in the state who is outside the state for a temporary or transitory purposes. How does this definition translate to the California Consumer Privacy Act (CCPA)?

A: The CCPA is concerned with personal information on California residents where some part of the business takes place in California. For example, if an individual lives in Los Angeles and orders something online from a retailer, and they ship it to California, that transaction would be within the scope of the CCPA. However, if an individual lives in Los Angeles and visits Detroit and buys something in person there, that would not be covered by CCPA.

Q: Is it correct that the CCPA does not apply to non-profit organizations' collection of personal information?

A: Correct, the CCPA defines a business as a for-profit business; non-profit organizations are exempt.

Q: Does 'sell data' refer to the actual sale of Personally Identifiable Information (PII), or just the use of PII throughout our organization and applicable vendors?

A: Because of the broad definition of 'sale', potentially all of the above. There are requirements that have to be dealt with just to collect data and anytime it goes to a third party, that would definitely be considered a sale. However, how the Attorney General's office enforces this portion of the law will reveal where exactly that line is, particularly as it relates to affiliated companies.

Q: Would 'harm' be recognized under the negligence standard as the time, money, and effort it takes to take back control of personal data (for example, if leaked information was used to steal an identity)?

A: Yes, it could be, however at this point, there have been so many breaches that the ability to prove that an identity was stolen as a direct result of a specific company's breach is almost impossible. So while that would be considered harm, it probably will not come into play very often because it is so hard to show.

Q: Under the CCPA, would de-identified data need to be also not able to be tied to a household/device (as opposed to not just being tied to a person)?

A: While on the webinar, it was said that data would need to be completely de-identified so that it could not be tied to a device, household, or person – this was incorrect. The actual CCPA de-identification language focuses on linking to an individual only. HITRUST® suggests using the Expert Method to ensure that all information is appropriately de-identified. For more information about de-identifying data and the Expert Method, take a look at the HITRUST® De-Identification Framework.

Q: Can the 10-day confirmation notification be an automated response email, or does it need to be more customized on a per-case basis?

A: It could be either; there is no prohibition on making the notification more customized, but it is certainly not required.

Q: If a non-profit 'sells' consumer data to another for-profit business or another non-profit entity, is that treated differently?

A: No; to be defined as a 'business' under CCPA the entity has to be for-profit, so while data is in the hands of the non-profit, CCPA is not applicable.

Q: If an organization chooses to add CCPA as a regulatory factor, do the added control requirement statements potentially have different implementation levels?

A: The 15 new CCPA-specific control requirement statements do not have various implementation levels. However, the four requirement statements which CCPA has been cross-mapped to may have varying implementation levels depending on the environment being assessed.

Q: HITRUST is clearly a good way to prove reasonable security protections, but is there a standard that the Attorney General (AG) will hold entities accountable to, such as CIS Top 20 or NIST?

A: The AG's office has not yet provided any guidance on 'appropriate and reasonable security' standards; in HITRUST's letter to the AG, we recommended that the AG's office recognize HITRUST and similar certifications.

Q: Is there a requirement for the number of 'clients' in CCPA?

A: With the assumption that the question is referring to the CCPA's definition of a 'business', a company which falls under CCPA's umbrella would do business in California and have a revenue of $25M or more, derive 50% or more of its annual revenues from selling data, or have information on 50K or more consumers, households, and/or devices. The 'client' requirement only becomes relevant if the revenue-related factors are not dispositive.

Q: Can a client create a CCPA-only assessment within the HITRUST MyCSF® platform?

A: Organizations with Corporate or Premier annual HITRUST MyCSF subscriptions can utilize the Custom Assessment feature to create a targeted assessment which includes only CCPA-related control requirement statements; these assessments cannot be submitted to External Assessor organizations for validation nor to HITRUST for the purpose of obtaining a formal report. For assessments that are intended to be submitted to HITRUST, CCPA can only be added as a regulatory factor.

Q: If an organization has many data processors, will it need to review its contracts to make sure they are CCPA-friendly?

A: In terms of contracts with service providers under CCPA, HITRUST would strongly recommend that organizations work with legal counsel to ensure the language in the contract provides what you need, particularly since there are new requirements about giving access to information. As an example, a client may want the service provider to be required to give access to data and do so within a certain period of time.

Q: How will CCPA affect organizations that do not sell data but process data at the direction of data owners?

A: Assuming that this question is coming from a service provider, it would depend on how that relationship is set up; service providers will have to comply with contracts with data owners. The contract should outline what can and cannot be done with data and service providers would need to comply with that direction, including deletion and opt-outs.

Q: Is an individual able to be certified as a CCPA?

A: While a 'CCPA certification' does not currently exist, a sole proprietorship can be considered a business under CCPA and should be taking steps towards implementing appropriate measures to become compliant.

Q: What specific new controls/measures should HIPAA-compliant businesses put in place to also be CCPA-compliant?

A: The delta is going to be how organizations manage non-HIPAA data. HIPAA data is exempt, however other data, such as data pertaining to employee and service provider staff, could be affected by CCPA.

Q: How does CCPA apply to a non-profit Texas health system that participates in research with a for-profit sponsor that is based in California?

A: The devil here is in the details. CCPA businesses and the CCPA language itself differentiates between service providers and third parties. HITRUST recommends reviewing the specifics with legal counsel.

Q: If a company is a covered entity under HIPAA, it is exempt from CCPA; however, if the company has a website that can be seen by both patients as well as non-patients, but all data is treated equally, does the exemption still apply to non-patients?

A: Under the CCPA, Protected Health Information (PHI) governed by HIPAA is exempted. This does not relieve a HIPAA covered entity who meets the definition of a business under CCPA of the related obligations when the data is not PHI.