

Does the California Consumer Privacy Act (CCPA), effective January 1, 2020, apply to my Organization?

- Is the organization a for-profit entity that collects personal information from California residents?

YES.

NO.

Be prepared in case the CCPA applies to the Organization in the future.*

Do one or more of the following requirements apply?

- Organization has annual gross revenues in excess of \$25 million dollars 
- Organization, alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices
- Organization receives 50 percent or more of its annual revenues from selling consumers' personal information

YES.

NO.

?

Implement CCPA compliance measures:

- **Individual Rights**
 - Create information notices to individuals
 - Create protocols for requesting individuals to request data and request that data be erased 
 - Review marketing practices for the right to opt-out of sale of information and the right to receive services on equal terms, without discrimination
- **Security**
 - Conduct risk assessment and implement reasonable cybersecurity safeguards for protecting personal information by establishing Written Information Security Plan ('WISP') and Incident Response Plan ('IRP') 
- **Service Providers**
 - Manage 3rd party vendors through contractual review and implementing protocols
- **Modify Website Privacy Notice**
 - Inform consumers of their rights 
 - Inform consumers on the categories of personal information collected
 - Inform consumers how the information will be used (including whether it will be shared with 3rd parties)
 - Include toll-free number or a physical address and email address for consumer requests

Does the Organization meet the following such that it is exempt from the CCPA's provisions? 

- Is it a health care provider that is regulated by the Health Insurance Portability and Accountability Act?
 - See Cal. Civ. Code § 1798.145(c)(1)(A); 45 C.F.R. § 160.103; 45 C.F.R. § 164.503(e).
- Is it a non-profit that does not operate for "profit or financial benefit?"
 - See Cal. Civ. Code § 1798.140(c)(1).
- Is it a consumer reporting agency that is regulated under the Fair Credit Reporting Act?
 - See Cal. Civ. Code § 1798.145(d); 15 U.S.C. § 1681(a).
- Is it a financial institution that is regulated under the Gramm-Leach-Bliley Act?
 - See Cal. Civ. Code § 1798.145(e); 15 U.S.C. §§ 6801–6809.

YES.

NO.

UNSURE?

1) Does Organization collect any information that falls outside scope of exemption?

YES.

2) Track CCPA amendments to ensure Organization remains exempt from CCPA provisions in the future

NO.

Check regulations to determine whether Organization falls within definition of entities/providers exempt from the CCPA

Risk of non-compliance includes: 

- **Regulatory risk** Subject to fines for damages per consumer incident in the event of a breach of unencrypted PI
 - Subject to civil penalty by Attorney General
- **Reputational Risk**
 - Brand damage
 - Reduced customer confidence
 - Reduced employee trust
- **Financial Risk**
 - Fines/penalties
 - Failure to comply can result in fines between \$2,500 and \$7,500 per violation
 - Litigation costs
 - Loss of revenue
 - Increase in cost of insurance

*Organization may want to take precautionary measures by implementing comprehensive CCPA compliance programs.