Published on *The National Law Review* https://natlawreview.com

California's Senate Bill 41: The Genetic Information Privacy Act

Article By:

Stephnie A. John

Lara D. Compton

Our previous blog post on pending California privacy legislation included a prediction that has since materialized: Governor Newsom signed the Genetic Information Privacy Act ("GIPA") on October 6, 2021, and the law will go into effect on January 1, 2022. GIPA establishes a number of mechanisms to close the existing gap in the protection of genetic information under the current framework of federal and state privacy laws. As discussed in our earlier post, GIPA contains a robust penalty structure, but it includes a number of carve-outs and does not apply to entities already subject to regulation under other health information privacy laws. Notably, GIPA does not reduce or eliminate obligations under other laws, including California's more broadly applicable consumer privacy laws, such as the CCPA and breach notification statute, as recently amended by AB 825. Given Governor Newsom's former concern about GIPA's interference with mandatory COVID-19 testing reporting, the law also does not apply to tests that are conducted exclusively to diagnose whether an individual has a specific disease.

Our prior posts explain the "genetic data" subject to the law and describe the direct-to-consumer genetic testing companies ("DTC Companies") that will need to comply with the new law. In this post, we discuss the requirements that will apply to DTC Companies in more detail.

Consumer Consent for Collection, Use, and Disclosure of their Genetic Data

In order to bridge the gap between the privacy requirements for DTC Companies who have historically avoided significant restrictions on the use and disclosure of genetic data and companies already subject to health information privacy laws (*e.g.*, HIPAA and/or the California Confidentiality of Medical Information Act), GIPA requires DTC Companies to obtain a consumer's express consent for each of the following actions:

- The use of genetic data collected through a genetic testing product or service offered by the DTC Company. The consent must describe who has access to genetic data, how genetic data may be shared, and the specific purposes for which it will be collected, used, and disclosed.

- The storage of a consumer's biological sample after the consumer's initial testing has been

completed.

- Each use of the consumer's genetic data or biological sample beyond uses associated with the primary purpose of the genetic testing or service.

- Each transfer or disclosure of the consumer's genetic data or biological sample to a third party other than to a service provider.

    - The consent must include the name of the third party to which the consumer's genetic data or biological sample will be transferred or disclosed.

- Marketing directed towards a consumer based on the consumer's genetic data, or the company's facilitation of marketing by a third party based on the consumer's order, purchase, or use of a DTC Company's genetic testing product or service.

Additionally, DTC Companies must provide consumers with straightforward methods of revoking their consent to the actions listed above at any time. Once a consumer revokes their consent, the company must honor this consent within 30 days of the revocation, including destroying biological samples. GIPA's requirement of a consumer's express consent is intended to target what is viewed as predatory practices of securing consumers' genetic information through inaction when a consumer forgets or is unaware their genetic information may be used unless they take specific action, and ensure a DTC Company does not use genetic data without obtaining consumers' adequately-informed permission.

Permissible Advertising

GIPA does not prevent DTC Companies from marketing directly on the Company's own website or mobile application to those consumers who have purchased or used their own genetic testing product or service, but it does place restrictions on the use of the wealth of information that DTC Companies can collect about consumers for marketing and advertising purposes. DTC Companies may generally market their services to existing customers without express consent, but they may not use any other information that they may have gleaned about a consumer to engage in more targeted advertising. Specifically, DTC Companies may not tailor their marketing practices on the basis of a consumer's sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, sexual orientation, citizenship, primary language, or immigration status.

While GIPA does not prohibit third-party advertising, DTC Companies must ensure that any advertisement of a third-party product or service be prominently labeled as advertising materials, including the name of the third-party who placed the advertisement. The third-party advertisement must clearly indicate if the advertised product or service, and any associated claims, have not been vetted or endorsed by the DTC Company.

DTC Companies and Service Providers

GIPA defines a "service provider" to be any entity involved in the "collection, transportation, and analysis of the consumer's biological sample" on behalf of DTC companies, or on behalf of any other company that collects, uses, maintains, or discloses genetic data collected from a direct-to-consumer genetic testing product or service, or arranges for the delivery of the results of the analysis of the biological sample or genetic material. DTC Companies must ensure their contracts with services

providers prohibit retaining, using, or disclosing genetic information for any other purpose other than the purpose of performing services to the DTC Company as specified in their contract. Specifically, the contracts must include provisions prohibiting service providers from the following:

- Retaining, using, or disclosing the biological sample, extracted genetic material, genetic data, or any other information regarding the identity of the consumer, including whether that consumer has solicited or received genetic testing, for a commercial purpose other than providing the services specified in the contract with the DTC Company; and

- Associating or combining the biological sample, extracted genetic material, genetic data, or any information regarding the identity of the consumer, including whether that consumer has solicited or received genetic testing, with information the service provider has received from other individuals, or has collected from its own interaction with consumers, or as required by law.

As further discussed below, DTC Companies may want to include additional contractual provisions to ensure compliance with the new law more broadly and may want to consider including indemnity provisions for violations of GIPA.

Patient Rights to Access and Delete

Under the new law, DTC Companies are required to develop policies and practices to enable consumers to easily do any of the following:

- Access their own genetic data;

- Delete their account and genetic data, with the exception of genetic data that must be retained pursuant to legal or regulatory requirements; and

- Arrange to have their biological sample destroyed.

To the extent relevant to service providers, DTC Companies may wish to flow down these requirements in their contracts.

Transparency Regarding the Use and Disclosure of Genetic Data

To ensure that consumers make an educated choice about whether or not to share their genetic data, DTC Companies must provide consumers with easily accessible privacy notices that contain the following information:

- A summary of its privacy practices that describes the company’s collection, use, maintenance, and disclosure of genetic data;

- Comprehensive explanations of the company’s data collection, consent, use, access, disclosure, maintenance, transfer, security, and retention and deletion practices;

- How to file a complaint alleging a GIPA violation with California’s Attorney General or other authorized state official as applicable; and

- A description of how de-identified genetic or phenotypic information may be shared with or disclosed to third parties for research purposes in accordance with federal regulations.

By requiring DTC Companies to provide notice of their privacy policies and practices, GIPA increases the level of accountability and transparency owed to consumers and opens the door for consumers and consumer protection agencies (including the Federal Trade Commission) to take action against DTC Companies in the event that consumers have been misled regarding the use and disclosure of their genetic data.

With respect to service providers, DTC Companies should be transparent about the service providers that they use, and consider whether their contracts should explicitly state that service providers may not use or disclose genetic data in violation of the company's consumer privacy notice.

Security Procedures for Storing Genetic Data

GIPA requires DTC Companies to implement "reasonable" security procedures and practices to protect consumers' genetic data against unauthorized access, destruction, use, modification, or disclosure. While the new law does not provide specifics on what would be considered reasonable, we note that the Assembly Committee on Privacy and Consumer Protection described HIPAA as "fairly robust" in finding that an exemption to GIPA requirements for entities subject to HIPAA was appropriate. As a result, compliance with the HIPAA Security Rule would likely be considered "reasonable" and practices that fall short of meeting those requirements may not. As a result, while not specifically required by the law DTC Companies should, as part of their compliance with these requirements, consider requiring service providers to meet specified security requirements and implement security procedures that are consistent with industry best practices by contract.

Additional Consumer Protections

GIPA protects consumers from discrimination based on the exercise of their rights under the Act. GIPA also prohibits DTC Companies from disclosing a consumer's genetic data to any entity responsible for administering health insurance, life insurance, long-term care insurance, or disability insurance. In order to avoid compliance missteps, DTC Companies may want to explicitly spell out these requirements in their service provider contracts.

DTC Companies should proactively review the requirements we have discussed, and prepare the forms, policies and procedures, and employee training that will be required to remain compliant with the new law.

National Law Review, Volume XI, Number 292