JULY 2025

FACT SHEET

Direct-to-Consumer Genetic/DNA Testing: Actions Consumers Can Take to Protect their Health Data

With the direct to consumer (DTC) genetic/DNA testing company 23andMe filing for Chapter 11 bankruptcy protection, the security of the information it holds on 15 million individuals has been called into question. Congress, the Federal Trade Commission (FTC), consumer groups, and others have raised concerns regarding how best to maintain the confidentiality of consumer genetic/DNA information. Laws aimed at protecting this type of genetic/DNA information, such as the Health Insurance Portability and Accountability Act (HIPAA), often do not apply to these private companies. The following is information consumers can use to take action to protect their data.

WHAT IS DTC GENETIC/DNA TESTING?

DTC genetic/DNA testing allows individuals to access genetic information without needing a health care provider. Online testing companies include: 23andMe, AncestryDNA, and MyHeritage.

Individuals typically collect a cheek swab or saliva sample and send it to the company lab to analyze. The vendor may provide genetic data (related to chromosomes or genes) as well as non-genetic data (blood biomarkers).

Some advanced testing packages include blood testing as well. Results typically take a few weeks and are returned to a secure website. Most companies have software and personalized genotyping reports or recommended consumer actions.

Information provided to the consumer can include ancestry, traits, and health-related issues. With many vendors, consumers can decide the scope of what is tested (i.e., health alone, ancestry alone, or a combination.)

DATA PRIVACY ISSUES SPARKED BY 23ANDME FILING FOR CHAPTER 11 BANKRUPTCY PROTECTION

Around 21% of Americans have taken a mail-in genetic/DNA test from a DTC testing company. The absence of privacy protections allows for the potential selling of American's data, posing a risk to consumers and the country's national security if a bad actor obtains the information.

Reason for 23andMe Bankruptcy: The company faced slowing sales, experienced a significant data breach in 2023 affecting 6.9 million users, and incurred financial settlements related to the breach.

Leadership Changes: Co-founder Anne Wojcicki stepped down as CEO as the company sought a buyer.

Impact on Users: Customers were advised by 23andMe to download their data and consider deleting their accounts if they are concerned about data privacy. The company has stated there are no immediate changes to how it stores, manages, or protects customer data.

Response from 23andMe: Of note is the recognition and affirmation from 23andMe that they will:

a. Commit to ensuring their customers have access to their genetic data, and 23andMe's protection of said data, and
b. In the event of a merger and acquisition or bankruptcy, their customers data may/will be sold to another entity BUT the original protection and access commitment will contractually be transferred to the new entity.

Recent Federal Action

- The FTC sent a letter on Mar. 21, 2025, to 23andMe raising concerns with the bankruptcy and genetic data privacy**.**
- On April 8, 2025, Bill Cassidy, MD (R-LA), Chairman of the Senate Committee on Health, Education, Labor, and Pensions sent a letter to 23andMe, raising concerns regarding data privacy.
- Senators Cassidy and Gary Peters (D-MI) introduced **Genomic Data Protection Act** (S.863) intended to give Americans using DTC genetic/DNA tests the choice to delete their genomic data and destroy their biological samples.

Current Federal Law

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The HIPAA Privacy Rule applies to health plans, providers of care, and health data clearinghouses (known as “covered entities”) and set national standards to protect medical records and other forms of paper and electronic protected health information (PHI), required safeguards to protect the privacy of PHI, sets limits and conditions on the uses/disclosures of PHI without authorization, as well as other consumer rights and protections. As 23andMe (and other DTC genetic/DNA testing vendors are not “covered entities,” HIPAA protections **do not apply** to the data they hold.

The HIPAA Security Rule protects electronic PHI by requiring covered entities to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability (CIA) of electronic PHI. This regulation: (i) protects individuals against discrimination based on genetic information in health insurance coverage and in the workplace, including employment opportunities; and (ii) safeguards individual and family privacy of genetic information.

Genetic Information Nondiscrimination Act (GINA)

GINA, passed in 2008, ensures that Americans are protected against discrimination by their employers or insurance companies based on genetic information in most situations. GINA, however, **does not extend** to genetic information-based discrimination in life, long-term care, or disability insurance providers. Under GINA, American insurance companies and health plans (including both group and individual insurers, as well as federally-regulated plans) are prohibited from: (i) looking at your predictive genetic information or genetic services before you enroll; (ii) "requesting or requiring" that you or your family members take a genetic test; (iii) restricting enrollment based on genetic information; and (iv) changing your premiums based on genetic information.

GINA also prohibits U.S. employers (including employment agencies, labor organizations, and training programs) from: (i) discriminating against who they hire or how much they pay on the basis of genetic information; (ii) "requesting or requiring" that you or your family members take a genetic test; and (iii) disclosing your genetic information in their possession except under specific and specially controlled circumstances.

Note that until the law is tested in court, it is difficult to know how far its protections will extend in practice.

Consumers should also be aware that many states also have their own laws prohibiting or at least limiting genetic discrimination. In California, for example, individual and group insurers are prohibited from requiring an individual to provide genetic information, from using genetic information to decide eligibility or risk status, and from disclosing such information without consent.

The American Society of Human Genetics provides an excellent lay person explanation of this law.

Federal Trade Commission Act

The FTC Act prohibits companies and individuals from engaging in unfair or deceptive acts or practices in or affecting commerce. The definition of health information goes beyond treatment and diagnoses and pertains to any information relating to a consumer’s health. The FTC Act seeks to:

- Prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce
- Seek monetary redress and other relief for conduct injurious to consumers
- Prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices
- Gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce
- Make reports and legislative recommendations to Congress and the public

Action Steps for Purchasers of DTC Genetic/DNA Testing

1. **ACT NOW!**
2. **DO NOT RELY ON:**
   a. The DTC genetic/DNA test company to manage and ensure your privacy of your genetic and health-related information
   b. Laws and regulations. These DTC genetic/DNA testing companies may not be subject to Federal or state privacy laws to protect you, such as:
      i. HIPAA
      ii. GINA
3. **ASSESS** the information you received in the DTC genetic/DNA test kit for any details on how they use or could use your genetic or health-related information, how they keep your information secure and private, how they protect your information from being inappropriately disclosed data protection, other rules, and other resources.
4. **REVIEW** the privacy policy from any other DTC genetic/DNA testing companies you may be a customer of for any potential data disclosure or privacy/security implications.
5. **CONTACT** the DTC genetic/DNA testing company immediately and demand IN WRITING that they delete your data completely from their database and all archived repositories.
6. **CHECK** your state's laws on consumer data privacy to see if you have any additional protection.

   For example, the California Privacy Protection Act (CPPA) provides California residents more control over their personal information collected by businesses about them.

   In the last few years, at least 11 states (including Arizona, California, and Maryland) have passed the Genetic Privacy Information Act, which governs data collection, use, security and disclosure requirements on DTC genetic/DNA testing companies and provides consumers with access and deletion rights, thus affording stronger protection on consumer genetic data.