Privacy Best Practices for Consumer Genetic Testing Services

July 31, 2018

1400 Eye Street, NW, Suite 450
Washington, DC 20005
fpf.org

Table of Contents

Introduction

Consumer genetic and personal genomic testing are tests that are marketed to Consumers by private companies. This type of testing has increased Consumers' access to and control of their Genetic Data; empowered Consumers to learn more about their biology and take a proactive role in their health, wellness, ancestry, and lifestyle; and enhanced biomedical research efforts. The consumer genetic and personal genomic testing industry is producing an unprecedented amount of Genetic Data, which provides the research community the ability to analyze significantly larger and more diverse range of Genetic Data to observe and discover new patterns and connections. It also enables researchers to gain a better understanding of the role of genetic variation in our ancestry, health, well-being, and much more.

Today, more consumer genetic and personal genomic testing services are available than ever before, prices for testing are becoming increasingly affordable, and the speed at which testing is completed is accelerating. As the industry continues to expand and the technology becomes more accessible, it is vital that the industry acknowledges and addresses the risks posed to individual privacy when Genetic Data is generated in the consumer context. Given the potential benefits that consumer genetic and personal genomic testing can provide to Consumers and society, it is important that this data is subject to privacy controls and used responsibly.

The Best Practices provide a policy framework for the collection, retention, sharing, and use of Genetic Data generated by consumer genetic and personal genomic testing services. These services are commonly offered to Consumers for testing and interpretation related to ancestry, health, wellness, genetic relatedness, lifestyle, compatibility, and other purposes. This document applies to Genetic Data, as defined in Annex A, which includes any data that concerns information about an individual's inherited genetic characteristics, including at least Raw Data, the Report of the Analyzed Data, and Self-Reported Health Data.[1]

This document recognizes that Genetic Data is sensitive information that warrants a high standard of privacy protection because of the following reasons:

- It may be used to identify predispositions, disease risk, and predict future medical conditions;
- It may reveal information about the individual's family members, including future children;
- It may contain unexpected information or information of which the full impact may not be understood at the time of collection; and
- It may have cultural significance for groups or individuals.

The Best Practices set a baseline of responsible practices intended to support a targeted Fair Information Practice Principles (FIPPs)[2]-based framework to address the privacy issues

[1] *See infra* Annex A (defining relevant terms related to Genetic Data)

[2] The FIPPs articulate basic protections for handling personal data and serve as a common language of privacy and a basis for law, regulation, and international agreements. These high-level guidelines were first articulated in 1973 by the United States Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems. They were codified in 1980 by the Organizations for Economic Cooperation and Development (OECD) and over time have been presented in different ways

related to the collection, retention, use, sharing, and research based on Genetic Data. The principles covered in these Best Practices include: (1) Transparency; (2) Consent; (3) Use and Onward Transfer; (4) Access, Integrity, Retention, and Deletion; (5) Accountability; (6) Security; (7) Privacy By Design; and (8) Consumer Education. By developing these responsible guidelines, we hope to ensure continued innovation and consumer trust within the consumer genetic and personal genomic testing industry.

Relevant legislation such as the Health Insurance Portability and Accountability Act (HIPAA), the Genetic Information Nondiscrimination Act (GINA), the Gramm-Leach-Bliley Act (GLBA), the Clinical Laboratory Improvement Amendments (CLIA), the Americans with Disabilities Act (ADA) and others may apply, and companies should reflect compliance with those and other applicable laws.[3] Privacy practices for non-genetic/genomic data are not addressed by these Principles, and, should reflect best practices along with applicable federal and state legal and regulatory privacy requirements.

♦ ♦ ♦

with different emphases. *See* Robert Gellman, *Fair Information Practices: A Basic History* (Apr. 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[3] *See infra* Annex B (listing primary applicable laws and regulations).

Privacy Best Practices for Consumer Genetic Testing Services

I. TRANSPARENCY: *Provide clear and complete information regarding the Company's policies and procedures for the management of personal data (personally identifiable information, Genetic Data, and protected health information) and de-identified information.*[4]

a. **Privacy Notices:** Privacy policies should be prominent, publicly accessible, and easy to read. They should specify the Company's data collection, consent, use, onward transfer, access, security, and retention/deletion practices.
   i. A high-level overview of the key principles should be provided preceding the full privacy policy. This overview should be a short document or statement that provides basic, essential information about the Company's collection, use, and sharing of Genetic Data.
   ii. Policies that vary for different categories of data should clearly spell out when each applies. For example, if the policy for Genetic Data is different than that of other data (e.g. registration data, browsing (cookies or website) tracking, and/or personal information), these policies should be described clearly and separately.

b. **Deidentification and Genetic Data**: Deidentified information is not subject to the restrictions in this policy, provided that the deidentification measures taken establish strong assurance that the data is not identifiable.
   i. We note that currently, Genetic Data held *at the individual-level* that has been de-identified[5] cannot be represented as strongly protecting individuals from re-identification, based upon existing deidentification tools and standards.[6] Such data may be protected in other ways and used for research with appropriate consent and security controls (See Principle VI: Security, below).
   ii. Aggregation of individual reports may provide strong assurance that personal data is not identifiable, if appropriate safeguards are in place.[7]

---

[4] *See infra* Annex A (defining "deidentified information").

[5] *See, e.g.,* U.S. Dep't Health & Hum. Services, Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (Nov. 26, 2012), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (presenting guidance for the HIPAA Safe Harbor Method).

[6] Commercial, technical protections and capabilities are currently being developed, but to date, protections for genetic data include strong security protocols, including removal of quasi-identifiers (demographic and other personal health information); retention separate from or without matching datasets; encryption; access controls; and contractual restrictions on sharing and use. Without a corollary dataset for matching, the risks remain minimal.

[7] The Federal Trade Commission (FTC) has identified its standards for reasonable de-identification for the protection of Consumer data, encompassing three steps: 1) reasonably deidentify the data using available practices to an extent appropriate to the sensitivity of the data, 2) commit to not attempting to re-identifying data, 3) when sharing deidentified data, contractually prohibit additional parties from attempting to reidentify (and monitor compliance). *See* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of*

c. **Policy Change**: Policies should indicate that material changes will not be made without first providing prominent notice and obtaining Consumer consent before data is used in any manner inconsistent with terms initially provided.

d. **Transfer of Ownership**: Policies should indicate that in the case of merger or acquisition by another entity, the successor entity is subject to these same commitments for the Genetic Data and biological sample already collected.[8]

e. **Transparency Reporting:** Companies should provide a public report describing requests from law enforcement for Genetic Data. Such reports should be made on at least an annual basis.[9]

II. CONSENT: *Obtain express consent for collection, analysis, sharing, or reporting of Genetic Data.*

a. ***Initial Express Consent*:** Initial express consent must describe data collection and uses of the commercial genetic product or services purchased by the Consumer, including the inherent contextual uses. Inherent contextual uses—such as providing the specific genetic analysis product or service, data use for product and service review and improvement, or new product development—should be clearly defined. Companies should clearly specify the uses of the Genetic Data, who will have access to test results, and how that data will be shared.

b. **Separate Express Consent:**[10] Separate express consent will be required for:
   i. Onward transfer of individual-level information (i.e., Genetic Data and/or personal information about a single individual) to third-parties for any reason, excluding vendors and service providers;[11]

Rapid Change (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
Under the HIPAA Privacy Rule, there are no restrictions on the use or release of deidentified data. Data is deidentified if it neither identifies nor provides a reasonable basis to identify an individual. This can be accomplished either by an expert determination using generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (or a HIPAA-specific Safe Harbor option based on removing enumerated fields). *See* U.S. Dep't Health & Hum. Services (HHS), *Summary of the HIPAA Privacy Rule* (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[8] The FTC has addressed both "material change" and "merger or acquisition" data use issues in its enforcement actions, and has made clear that it could be an unfair practice under Section 5 for a company to alter its privacy policies in a way that's inconsistent with the promises made when the information was collected, without notice and new consent. *See* Jamie Hine, Fed. Trade Comm'n, *Mergers and Privacy Promises* (Mar. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

[9] Peter Micek, *Transparency Reporting Index*, Access Now (2016), https://www.accessnow.org/transparency-reporting-index/.

[10] Express consent means a Consumer's statement or clear affirmative action in response to a clear, meaningful, and prominent notice regarding the collection, use, and sharing of data for a specific purpose.

[11] Vendors and service providers are companies that act under the direct authority of the data controller or processor and are authorized to process personal data in support of providing the data controller's commercial product or service. For the purposes of this document, a company's vendors and service providers are not third parties, provided that appropriate contractual controls bind such vendors and service providers.

ii. Incompatible secondary uses[12] of Genetic Data; and
iii. Consumers or organizations that submit biological samples or Genetic Data on behalf of other individuals (others, elderly relatives, etc.).
    a) Policies should require that the individual submitting the Biological Sample or the Genetic Data is the owner or include reasonable steps to ensure that consent has been obtained from the owner of the Biological Sample or Genetic Data.[13]

c. **Informed Consent for Research:**[14] Informed consents should include basic elements,[15] such as an acknowledgment of the voluntary nature of the research, a statement concerning the confidentiality of data, and a description of risks, benefits, and purpose of the research. Informed consent will be required when:
    i. Genetic Data is transferred to third parties for research purposes; and
    ii. Research is done under the control of the Company (i.e. internal research) for the purpose of publication or generalizable knowledge (this excludes product development, quality control, or data processing to support inherent contextual uses), unless otherwise approved by an institutional review board (IRB)[16] or internal ethical

---

[12] Incompatible secondary uses include those uses outside of the primary purpose of the purchased service and the inherent contextual uses. Incompatible secondary uses do not include activities intended to develop or improve new or current products.

[13] With regard to minors or those incapacitated, appropriate permissions to submit a Biological Sample or Genetic Data on behalf of another may vary from consent, power of attorney, guardianship, etc., depending on the nature of the relationship between the Data/Sample owner and the Data/Sample submitter.

[14] Informed consent is the process of providing an individual with adequate information about the research to allow for an informed decision about the individual's voluntary participation in a research study.

[15] According to the HHS Office of Research Protections, the 8 basic elements of an informed consent include:

A. "a statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures which are experimental;
B. a description of any reasonably foreseeable risks or discomforts to the subject;
C. a description of any benefits to the subject or to others which may reasonably be expected from the research;
D. a disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject;
E. a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained;
F. for research involving more than minimal risk, an explanation as to whether any compensation and an explanation as to whether any medical treatments are available if injury occurs and, if so, what they consist of, or where further information may be obtained;
G. an explanation of whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject; and
H. a statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled."

Additional elements of informed consent may apply. Additional elements of informed consent may apply. *See* 45 C.F.R. § 46.116 (2009), https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html#46.116.

[16] An IRB is a group designated to review research protocols and related materials (including informed consents) and assure that appropriate steps have been taken to protect the rights and welfare of human research subjects. IRBs have the authority to approve, modify, or disapprove research. See 45 C.F.R. § 46.107–115 (2009), https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html.

review process.[17]

d. **Marketing:**[18] Companies should provide Consumers with the ability to opt-out of communications from the Company, excluding communications that provide information about the maintenance of accounts or related to an ongoing product or service provided
    i. Marketing to a Consumer based on Genetic Data is not permitted, unless the Consumer has provided separate express consent for such marketing or otherwise is clearly described in the initial express consent as a primary function of the product or service.
    ii. Marketing to a Consumer because they have ordered or purchased a genetic product or service is not permitted, unless the Consumer has been provided the ability to opt-out of such marketing.
    iii. Marketing to any individual is not permitted when based on (a) the Genetic Data of a Consumer who is a relative or (b) the order or purchase of a genetic product or service by a Consumer who is a relative.[19]
    iv. Marketing does not include the provision of customized content or offers by the Company on its own websites and services.

e. **Minors' (Under 18) Genetic Data:** Consumer-facing services should not be marketed to, or offered directly to anyone under the age of 18.
    i. Processing and analysis of samples and account activation for those under 18 may be provided with the consent of a parent or guardian.
    ii. Companies should provide a method for minors to be provided access to their Genetic Data and to become the primary holder of their account after they reach the age of 18.

---

[17] An ethical review process (also referred to as a corporate IRB, Consumer subject review board, or corporate ethics boards) has been proposed for the ethical review for data that is not typically covered by the Common Rule. The purpose of these reviews is to identify both the risks and the benefits of the research and to balance the prospective risks to the Consumer, prospective benefits to Consumers or to the public, the rights and interests of the Consumer, and the legitimate interests of the company. See Dennis D. Hirsch, et al., *Roundtable: Beyond IRBs: Designing Ethical Review Processes for Big Data*, 72 Wash. & Lee L. Rev. Online 406–498 (2016), https://scholarlycommons.law.wlu.edu/wlulr-online/vol72/iss3/; Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 Stan. L. Rev. Online 97 (Sept. 2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards.

[18] Under the HIPAA Privacy Rule, marketing is defined as "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Covered entities must obtain written authorization for any use or disclosure of PHI for marketing communications, except those in-person or which involve a promotional gift of nominal value. HIPAA exempts certain types of communications from the definition of marketing, such as communications made (1) for treatment of the individual; (2) for case management or care coordination, or to direct or recommend alternative treatments, therapies, providers, or settings; and (3) to describe health-related products or services provided by the covered entity or included in a plan of benefits. For example, "a hospital's Wellness Department could start a weight-loss program and send a flyer to all patients seen in the hospital over the past year who meet the definition of obese, even if those individuals were not specifically seen for obesity when they were in the hospital," because the wellness program is about the covered entity's own health-related service. *See* U.S. Dep't Health & Hum. Services, Office for Civil Rights, *Marketing [45 CFR 164.501, 164.508(a)(3)]* (Apr. 3, 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[19] "Refer a friend" communications or communications that facilitate a Consumer's sharing of results and recommending the purchase of products or services to others are not covered by this section.

III. USE AND ONWARD TRANSFER: *Commit to collecting, using, and sharing Genetic Data in ways that are compatible with reasonable Consumer expectations for the context in which the data was collected.*

a. **Prohibited Sharing:** Genetic Data, by definition linked to an identifiable person, should not be disclosed or made accessible to third parties, in particular, employers, insurance companies, educational institutions, or government agencies, except as required by law or with the separate express consent of the person concerned. (See Principle IV(d): Law Enforcement Access, below)

b. **Vendors/Service Providers:** Companies are responsible to ensure that any vendors and service providers are bound to the same level as the Company's privacy commitments under these Principles, and the associated policies, and such partners have no independent rights to use Genetic Data or other personal information outside the scope of their role in providing the primary product or service. In the case of a Company ending or selling its business, it should either dispose of Consumers' Genetic Data and Biological Samples securely, or ensure recipient third party commitments consistent with the original notices provided to the Consumer.[20]

c. **Research:** As discussed under "Principle II: Consent," sharing of individual-level Genetic Data with third parties for additional research should only be allowed with specific separate express consent or informed consent from the Consumer.[21]

IV. ACCESS, INTEGRITY, RETENTION, AND DELETION:

Provide the Consumer with access to their Genetic Data and inform the Consumer of what rights they have to correct or amend the record, how to report security concerns, and how long their Genetic Data and the original Biological Sample will be maintained.[22]

a. **Access:** Companies should provide a method for Consumers to access their Genetic Data through the services, as well as:
    i. Provide a process for Consumers to indicate the handling of their account, such as granting access, deletion, and/or transferring account control, in case of death or if a Consumer becomes incapacitated; and/or

[20] Per FTC guidance, effective vendor oversight includes: reasonable due diligence in selecting vendors; limiting shared data to those required by business needs; contractual requirement for vendors to ensure collection, use, and retention policies to protect PII; and most significantly, adequate monitoring of vendor privacy and security practices. The GDPR likewise clearly delineates responsibilities between "controllers" and "processors" for handling personal information, with responsibility and liability for Controllers as ultimate owners of the data. Controllers should: Only use processors that provide sufficient guarantees of their abilities to implement the technical and organizational measures necessary; Carry out data protection impact assessment prior to contract; Contractually ensure vendor compliance responsibilities and practices.

[21] Companies should take note of the range of guidance provided by organizations on data sharing practices (See Annex C: Genetic Data Sharing Policies, below).

[22] Retention and deletion/destruction policies should clearly identify practices regarding both the physical sample(s) provided, and the data derived or obtained from analysis of those samples.

ii. Implement a process for a successor to request the transfer of an account after the death or if a Consumer becomes incapacitated.

b. **Integrity:** Genetic Data should be maintained at an industry standard of accuracy.[23]

c. **Retention:** Companies should set reasonable practices for Genetic Data retention and data minimization, taking into account the existence of active Consumer accounts, inherent contextual uses, and regulatory retention requirements.[24]
   i. Retention practices should address both the Biological Sample provided and Genetic Data.

d. **Deletion:** Unless otherwise required by law,[25] Companies should provide Consumers clear and prominent methods to delete their account and Genetic Data and destroy their Biological Sample, and describe any relevant limitations.
   i. For Consumers who have agreed to an informed consent for research, companies may not be able to delete or remove their Genetic Data from active or completed research, or from published results and findings. If deletion is requested, Genetic Data should not be used for any future or new research.
   ii. Companies should remove or restrict access to Genetic Data when deletion is not possible due to legal or technological requirements or other limitations.

e. **Law Enforcement Access:** Genetic Data may be disclosed to law enforcement entities without Consumer consent when required by valid legal process.[26] When possible, companies will attempt to notify Consumers on the occurrence of personal information releases to law enforcement requests.[27] Companies

---

[23] Nat'l Human Genome Research Inst., *Regulation of Genetic Tests* (Jan. 17, 2018), https://www.genome.gov/10002335/regulation-of-genetic-tests

[24] For example, retention may be limited due to regulatory or accreditation requirements. The Clinical Laboratory Improvement Amendments (CLIA) require that a data be stored according to retention requirements for CLIA certified laboratories. *See infra* Appendix B, Section IV for more information about CLIA. The College of American Pathologists (CAP) Laboratory Accreditation Program was granted authority by the Centers for Medicare and Medicaid Services (CMS) to inspect laboratories performing testing on human or animal specimens in lieu of a CMS inspection. CAP accredited laboratories are required to retain certain documents and specimens for quality testing and assurance. Coll. of Am. Pathologists, *Laboratory General Checklist: CAP Accreditation Program* 19 (July 28, 2015), http://www.cap.org/ShowProperty?nodePath=/UCMCon/Contribution%20Folders/DctmContent/education/OnlineCourseContent/2016/LAP-TLTM/resources/AC-laboratory-general.pdf#page=19.

[25] *See infra* Appendix B, Section IV for more information about CLIA.

[26] If a Consumer has agreed to provide their data for research, Genetic Data may be subject to confidentiality protections. For federally funded research, the 21st Century Cures Act guards against inappropriate use of the Freedom of Information Act (FOIA) to gain access to participants' genetic information by allowing the Secretary of the Department of Health and Human Services (HHS) to disqualify such research data from FOIA requests if: "(A) an individual is identified; or "(B) there is at least a very small risk, as determined by current scientific practices or statistical methods, that some combination of the information, the request, and other available data sources could be used to deduce the identity of an individual." *See* 21st Century Cures Act, Pub. L. No. 114-255, § 2013, 130 Stat. 1033 (2016), https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf.

[27] HIPAA limits the type of information that covered entities may dislose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It

should consider the feasibility of applying for certificates of confidentiality for relevant research.[28]

V. ACCOUNTABILITY: *Designate a responsible office or official who is accountable for the organization's compliance with the Privacy Principles*.

a. **Enforcement:** Implement reasonable policies, procedures, and practices to ensure that these Principles guide the collection, use, sharing, and storage of Genetic Data by the Company. Provide public/consumer facing commitments that are enforceable by the FTC, State Attorneys General, or other authorities.

b. **Training:** Implement training programs for personnel who handle Genetic Data. Consider creating internal privacy review boards to evaluate and approve new technologies and services involving Genetic Data.

VI. SECURITY: *Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of Genetic Data against risks – such as unauthorized access or use, or unintended or inappropriate disclosure or breach – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.*

a. **Protection:** Genetic Data requires high levels of security and confidentiality. Genetic Data should be protected through a combination of mechanisms including, at a minimum: secure storage of human biological materials and data, encryption of digital records, data-use agreements, and contractual obligations, and accountability measures (e.g. training, access controls and logs, and independent audits).

VII. PRIVACY BY DESIGN: *Implement technological controls that support or enforce compliance with these Principles in addition to policy, legal, and administrative measures.*

a. **Assessment:** Companies should undertake a comprehensive evaluation of the Genetic Data required at each step to ensure only appropriate data is collected and that reasonable Genetic Data retention practices are in place

---

specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. *See* U.S. Dep't Health & Hum. Services, Office for Civil Rights, *Will this HIPAA Privacy Rule Make It Easier for Police and Law Enforcement Agencies to Get My Medical Information?* (Dec. 20, 2002), https://www.hhs.gov/hipaa/for-individuals/faq/349/will-hipaa-make-it-easier-for-law-enforcement-to-get-my-medical-information/index.html.

[28] For non-federally funded research, investigators may apply for a certificate of confidentiality (CoC) through the NIH, as laid out in Section 2012 of the 21st Century Cures Act. CoCs protect the privacy of research participants by protecting identifiable health information from compelled disclosure. While CoCs are typically reserved for federally funded research, the NIH also considers requests for COCs for non-federally funded research in which identifiable, sensitive information is collected or used, including individual level human genomic data. *See* Nat'l Inst. of Health, Certificates of Confidentiality Kiosk, *Certificates of Confidentiality: Background Information* (2017), https://humansubjects.nih.gov/coc/background.

(see Principle IV(c): Retention, above).[29]

VIII. CONSUMER EDUCATION: *Make available to Consumers resources that advise about the implications and consequences of genetic testing, research, and data sharing.*

a. **Education:** Companies should inform Consumers about the basics of genetics and genetic testing; the risks, benefits, and limitations of genetic testing; and the appropriate interpretation and use of results.[30] Companies should do so by providing such materials themselves or pointing to appropriate third-party resources.

[29] *See, e.g.*, Fed. Trade Comm'n, *Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Commision Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG; Hugo Teufel III, U.S. Dept. of Homeland Security, Privacy Policy Guidance Memorandum (Memorandum No. 2008-01, Dec. 29, 2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[30] For FDA approved devices, other special controls may apply, such as requirements to include limiting statements about what genetic risk information the test does and does not provide and how other factors such as environmental and lifestyle risk factors may affect the risk of developing disease, among others. *See* 21 C.F.R. § 866.5950 (2018), https://www.ecfr.gov/cgi-bin/text-idx?SID=26b6a62c2603684a93b9bffa0095289a&mc=true&node=pt21.8.866&rgn=div5#se21.8.866_15950.

Annex A: Definitions

Biological Sample: Any material part of the human body, discharge therefrom, or derivative thereof, known to contain DNA, e.g. tissue, blood, urine, or saliva. Includes extracted DNA: the physical DNA material that has been isolated and purified from the original biological sample.

De-identified Information: Information that does not include direct or indirect identifiers such that information cannot reasonably be associated with an individual. Not limited to aggregated information.

Consumer: An individual who has ordered or purchased a Company's genetic product or service

Company: Any entity that offers consumer genetic and personal genomic testing products or services to Consumers

Genetic Data: Any data that, regardless of its format, concerns information about an individual's inherited or acquired genetic characteristics, including at least an individual's Raw Data, the Report of the Analyzed Data, and Self-Reported Health Data.[31]

- **Raw Data**: Data that results from the sequencing of an individual's complete extracted DNA or a portion of the extracted DNA. Sequencing is the process of identifying the order of the 4 chemical unites that compose DNA—adenine (A), thymine (T), guanine (G), and cytosine (C)—in an individual's complete DNA sequence (whole genome sequencing) or regions of the DNA sequence (targeted sequencing or genotyping).

- **Report of the Analyzed Data**: Data that results from analyzing the raw sequence data. This data typically includes genotypic and phenotypic information.

- **Self-Reported Health Data**: Information that an individual submits to the company regarding their health conditions that is used for scientific research or product development and analyzed in connection with that individual's Raw Data.

Genetic Testing: Any laboratory test of an individual's complete DNA, regions of DNA, chromosomes, genes, or gene products to determine the presence of the genetic characteristics in an individual or an individual's offspring.[32] Over 1,000 genetic tests currently used today. The results of a genetic test may include genotypic and phenotypic data.[33]

---

[31] The genome is the complete set of an individual's DNA, including all of its genes. A copy of the entire human genome contains more than 3 billion DNA base pairs. This data forms the basis for genomics, the study of how the genes within the genome interact with each other and with the individual's environment. A gene is a sequence of the genome that has a particular function. World Health Organization, *WHO Definitions of Genetics and Genomics*, http://www.who.int/genomics/geneticsVSgenomics/en/.

[32] MedlinePlus, U.S. Nat'l Library of Med., *Genetic Testing* (May 16, 2008), https://medlineplus.gov/genetictesting.html.

[33] Genetics Home Reference, *Help Me Understand Genetics: Genetic Testing* (July 10, 2018), https://ghr.nlm.nih.gov/primer/testing.pdf.

- **Genotypic Data:** Data about an individual's genetic sequence at particular locations at the genome, which determines in part the characteristics of an individual (the phenotype). This includes the A's, T's, C's, and G's at particular locations in the genome, either within a gene or outside of a gene.[34]

- **Phenotypic Data:** Data about the characteristics of an individual resulting from the expression of the genotype and its interaction with the environment. This includes an individual's physical, behavioral, and developmental traits, such as eye color, height, and blood type.[35]

Personal Information: All information, including Genetic Data, that can be used to identify or locate an individual, either alone or in combination with other information.

Protected Health Information: The term for protected data under HIPAA. Generally refers to demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care.[36]

Self-Reported Data: Information that an individual submits to the company through surveys, questionnaires, or online user interfaces directly linked to the individual.

---

[34] National Institutes of Health, National Human Genome Research Institute, Talking Glossary of Genetic Terms, https://www.genome.gov/glossary/index.cfm?id=93&textonly=true.

[35] *Id*.

[36] The HIPAA Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information PHI." *See* HHS *supra* note 7.

Annex B: Legal and Regulatory Guidance

I. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA lays out the privacy and security requirements for protected health information collected, processed, and used by covered entities (health plans, healthcare clearing houses, healthcare providers, business associates), as defined by the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"). Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties. The Privacy Rule protects all "individually identifiable health information" (protected health information) held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Under HIPAA, genetic information is considered health information, and covered entities are prohibited from using and disclosing genetic information for underwriting purposes. While all health plans are subject to this prohibition, long-term care plans are excluded. HIPAA requires written consent except for identified exceptions, including "purposes of research, public health or health care operations." "A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care."[37]

II. The Genetic Information Nondiscrimination Act of 2008 (GINA)

GINA is a federal law that protects individuals from genetic discrimination by health insurers (Title I) and employers (Title II). Title I of GINA also required HHS to revise the definition of health information to include genetic information. Under GINA, genetic information is defined as "any individual, information about (i) such individual's genetic tests, (ii) the genetic tests of family members of such individual, and (iii) the manifestation of a disease or disorder in family members of such individual." This information is treated as part of confidential medical record. An employer, employment agency, labor organization, or join labor-management committee should not disclose an employee's/member's genetic information except:

1. to the employee or member of a labor organization (or family member if the family member is receiving the genetic services) at the written request of the employee or member of such organization;
2. to an occupational or other health researcher if the research is conducted in compliance with the regulations and protections provided for under part 46 of title 45, Code of Federal Regulation" … (other limitations are listed for law enforcement, court orders, and compliance with other federal and state laws or regulations).[38]

III. The Americans with Disabilities Act (ADA)

The ADA is a federal law that prohibits discrimination on the basis of disability. The ADA prohibits discrimination based on disability in employment, public services,

---

[37] For more information about implementing HIPAA privacy requirements, please see: Office for Civil Rights. (2003). *See* HHS *supra* note 7.

[38] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2012), https://www.gpo.gov/fdsys/pkg/PLAW-110publ233/html/PLAW-110publ233.htm.

accommodations, and communications.[39] The Equal Employment Opportunity Commission (EEOC) issued an interpretation in 1995 of the ADA declaring that the ADA prevents employment discrimination based on genetic information related to illness, disease, or other disorders. This interpretation is non-binding.[40,41]

IV. Clinical Laboratory Improvement Amendments (CLIA) [42 USC 263a]

The Clinical Laboratory Improvement Amendments (CLIA) was passed in 1988 to regulate laboratory testing and requires that clinical laboratories become certified by their state and CMS before they can handle human samples for clinical purposes. Specifically, laboratories **must** obtain a CLIA certificate prior to testing when: (1) patient-specific results are reported from the laboratory to another entity; AND (2) the results are made available "for the diagnosis, prevention, or treatment of any disease or impairment of, or the assessment of the health of, human beings." To become certified, laboratories must demonstrate the accuracy, reliability, and timeliness of test results and handling of biological samples. Depending upon the testing conducted, CLIA requirements will vary. CLIA laboratories must maintain (1) test authorizations, (2) test procedures, (3) analytic systems records, (4) proficiency testing records, (5) quality system assessment records, and (6) test reports for at least 2 years. Depending upon the histopathology slide, pathology specimen block, or tissue analyzed, retention periods will vary.[42,43]

V. Code of Federal Regulations, Title 45, Part 46: Protection of Human Subjects (45 CFR 46)

The Office of Human Research Protections (OHRP) within the Department of Health and Human Services (HHS) considers human biological specimens or private information to be identifiable when they can be linked directly or indirectly to a specific individual, as defined by 45 CFR 46.102(f). As set out by 45 CFR 46.102(f), "obtaining identifiable private information or identifiable specimens for research purposes constitutes human subjects research. Obtaining identifiable private information or identifiable specimens includes, but is not limited to:

1. using, studying, or analyzing for research purposes identifiable private information or identifiable specimens that have been provided to investigators from any source; and

---

[39] Americans with Disabilities Act of 1990, 42 U.S.C. § 12101 (2012), https://www.congress.gov/bill/101st-congress/senate-bill/933.htm.

[40] Mark A. Rothstein, *GINA, the ADA, and Genetic Discrimination in Employment*, 36 J. Law Med. Ethics 837–840 (2008), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3035561/.

[41] Lewis Maltby, *Genetic Discrimination and the Americans with Disabilities Act: An Unlikely Fit*. National Workrights Institute (May 21, 1998), http://www.workrights.org/nwi_geneticTesting_geneticDiscr.html.

[42] Clinical Laboratory Improvement Amendments of 1988, 42 U.S.C. § 263a (2012), https://www.congress.gov/bill/100th-congress/house-bill/5471.

[43] 42 C.F.R. 493.1105 (2012), https://www.gpo.gov/fdsys/pkg/CFR-2011-title42-vol5/pdf/CFR-2011-title42-vol5-sec493-1105.pdf.

2. using, studying, or analyzing for research purposes identifiable private information or identifiable specimens that were already in the possession of the investigator."[44,45]

VI. General Data Protection Regulation (GDPR)

The GDPR is a regulation of the European Parliament, the Council of the European Union, and the European Commission that is intended to strengthen and unify data protection across the European Union. The GDPR was adopted on April 14, 2016 to replace the Data Protection Directive (95/46/EC) and came into effect on May 25, 2018. The GDPR specifically acknowledges that the definition of personal health data should include: "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from Genetic Data and biological samples**;** and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."[46]

VII. The Patient Protection and Affordable Care Act (ACA)

The ACA is a federal law that aims to extend health insurance coverage to Americans by expanding both private and public insurance, increase consumer protections, improve quality and system performance, control rising healthcare costs, and increase prevention and wellness initiatives. The ACA prohibits health insurance providers from discriminating against patients with genetic information by preventing coverage based on "pre-existing conditions" and requiring health insurers to provide coverage to all individuals who request it, as laid out in 42 USC § 2705(a)(6): "Prohibiting Discrimination Against Individual Participant and Beneficiaries Based on Health Status."[47]

VIII. The Gramm-Leach-Bliley Act (GLBA)

Also known as the Financial Modernization Act of 1999, the GLBA is a federal law that requires financial institutions, including insurance companies, to provide customers with notice about personal information use and sharing practices and to safeguard sensitive information. This personal information includes genetic information and other

---

[44] *See* 45 C.F.R. § 46 (2009), https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html.

[45] *See* U.S. Dept. of Health and Human Services, Office for Human Research Protections, *Coded Private Information or Specimens Use in Research, Guidance* (Oct. 16, 2008) https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html.

[46] Commission Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

[47] Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, 124 Stat. 119 (2010), https://www.gpo.gov/fdsys/pkg/PLAW-111publ148/html/PLAW-111publ148.htm

health information. As a result, health plans and health insurers are required to take a variety of actions with respect to the handling of member or subscriber data, in electronic format or otherwise.[48]

IX. State Laws and Regulations

States have passed a patchwork of laws to protect Americans from genetic discrimination. These laws vary widely in scope, applicability, and the amount of protection provided. Currently:

- 48 states and the District of Columbia prohibits genetic discrimination in health insurance;
- 35 states and the District of Columbia prohibit genetic discrimination in employment;
- 17 states prohibit genetic discrimination in life insurance coverage;
- 17 states prohibit genetic discrimination in disability insurance; and
- 8 states prohibit genetic discrimination in long-term care insurance.[49]

Further, the California Genetic Information Nondiscrimination Act (CalGINA) prohibits genetic discrimination in emergency medical services, housing, mortgage lending, education, and other state funded programs.[50]

---

[48] Gramm-Leach-Bliley Act Gramm-Leach-Bliley Act, 12 U.S.C. § 1811 (1999), https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

[49] Nat'l Human Genome Research Inst., *Genetic Discrimination and Other Laws* (Apr. 17, 2017), https://www.genome.gov/27568503/genetic-discrimination-and-other-laws/.

[50] *See* Nat'l Human Genome Research Inst., *Genome Statute and Legislation Database* (July 11, 2018), https://www.genome.gov/policyethics/legdatabase/pubsearch.cfm.

Annex C: Genetic Data Sharing Policies

I. OECD Guidelines on Human Biobanks and Genetic Research Databases

The OECD Recommendation on Human Biobanks and Genetic Research Databases was adopted in October 2009 by the OECD Council as a non-legally binding contract. The Guidelines "provide guidance for the establishment, governance, management, operation, access, use and discontinuation of human biobanks and genetic research databases ("HBGRD"), which are structured resources that can be used for the purpose of genetic research and which include: (a) human biological materials and/or information generated from the analysis of the same; and (b) extensive associated information." In relation to consent for secondary research, the Guidelines suggests that: "It is clear that wide access to such data and materials for biomedical advances must be balanced by concern for the interests of research participants (i.e. those individuals from whom biological materials and data are obtained). The ability to establish biobanks and genetic research databases will depend in part on participants' willingness to contribute. Research must respect the participants and be conducted in a manner that upholds human dignity, fundamental freedoms and human rights and be carried out by responsible researchers."[51]

II. Public Health Genomics European Network (PHGEN) II

PHGEN II produced the "European Best Practice Guidelines for Quality Assurance, Provision and Use of Genome-based Information and Technologies." These guidelines were created to assist Member States and EFTA-EEA countries with best practices for the responsible and timely integration of genetic into population health. PHGEN II recognizes the issue of expanding the affected parties beyond the primary data subject to include family members and states: "As an ethical and legal issue related to the privacy and rights over genome-based information it has been argued that the "data subject" concept could be put into question due to the hereditary feature of certain information which is of shared value for a family. Should the data subject only be the individual from which sample and data have been processed or should it be extended to family? Considering the rights attached to the data subject and the complexity that would trigger such extension, it is desirable to not modify this notion and to keep the individual definition of "data subject"."[52]

III. Global Alliance for Genetics and Health (GA4GH)

The Global Alliance for Genomics and Health is an international non-profit dedicated to improving human health by increasing the potential of genomics through effective and responsible data sharing. The GA4GH "Privacy and Security Policy" outlines policies for the sharing of genetic data in a way that promotes the confidentiality, integrity, and availability of data, and the privacy of individuals, families, and communities whose genetic data are shared. In particular, the policy notes that: "If data are Coded or Anonymized, it should take place at the earliest opportunity consistent with use for the authorized purposes. Moreover, Data Stewards should provide a clear summary or description of the coding or anonymization process that was applied…Such description

---

[51] Org. for Econ. Co-operation and Dev., *OECD Guidelines on Human Biobanks and Genetic Research Databases* (2009), https://www.oecd.org/sti/biotech/44054609.pdf.

[52] Public Health Genomics European Network, *European Best Practice Guidelines for Quality Assurance, Provision and Use of Genome-based Information and Technologies* (Apr. 2012), https://webgate.ec.europa.eu/chafea_pdb/assets/files/pdb/20081302/20081302_d06_en_ps.pdf.

should also make clear that if Data are Anonymized, further robust data linkage would not be possible." [53,54]

IV. NIH "Genomic Data Sharing (GDS) Policy" & "Policy for Sharing Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies (GWAS)"

The NIH GDS Policy applies to all NIH-funded research that generates large-scale human or non-human genomic data (controlled-access and unrestricted-access) as well as the use of data for subsequent research. It outlines practices to ensure the broad and responsible sharing of genomic research data. On sharing of deidentified data, the policy states: "NIH expects that informed consent for future research use and broad data sharing will have been obtained even if the cell lines or clinical specimens are de-identified" and that the "risk of re-identification must be conveyed to prospective subjects in consent process."[55] The NIH also created a "Policy for Sharing Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies (GWAS)," which recognizes that: "Although the NIH-held data will be coded and the NIH will not hold direct identifiers to individuals within the NIH GWAS data repository, the agency recognizes the personal and potentially sensitive nature of the genotype-phenotype data. Further, the NIH takes the position that technologies available within the public domain today, and technological advances expected over the next few years, make the identification of specific individuals from raw genotype-phenotype data feasible and increasingly straightforward."[56]

V. Welcome Trust Sanger Institute "Data Sharing Policy"

The Welcome Trust Sanger Institute is a non-profit British genomics and genetics research institute. The Data Sharing Policy" applies to genetic and genomic data generated at the Institute, released via either open or managed access. Specifically, the Welcome Trust Sanger Institute acknowledges the differing risk of reidentification for genetic information depending upon the data fields released, and list factors that can contribute to lowering the risk of re-identification.[57]

---

[53] Global Alliance for Genomics and Health, *Global Alliance for Genomics and Health: Privacy and Security Policy* (May 26, 2015), https://www.ga4gh.org/docs/ga4ghtoolkit/data-security/Privacy-and-Security-Policy.pdf.

[54] The GA4GH has also published a "Framework for Responsible Sharing of Genomic and Health-Related Data," which provides harmonized approached to enable effective and responsible genetic data sharing projects. *See* Global Alliance for Genomics and Health, *Framework for Responsible Sharing of Genomic and Health-Related Data* (Dec. 9, 2014), https://www.ga4gh.org/ga4ghtoolkit/regulatoryandethics/framework-for-responsible-sharing-genomic-and-health-related-data/.

[55] Nat'l Institutes of Health, *Genomic Data Sharing (GDS) Policy* (Aug. 27, 2014), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-14-124.html.

[56] National Institutes of Health, *Policy for Sharing of Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies (GWAS)* (Aug. 28, 2007), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-07-088.html.

[57] Wellcome Trust Sanger Institute, *Data Sharing Policy* (May 2014), https://www.sanger.ac.uk/sites/default/files/Jul2017/Data_Sharing_Policy_and_Guidelines_July_2017_0.pdf.

About the Future of Privacy Forum

The Future of Privacy Forum (FPF) is a catalyst for privacy leadership and scholarship, advancing responsible data practices in support of emerging technologies. FPF is based in Washington, DC, and includes an advisory board comprised of leading figures from industry, academia, law, and advocacy groups.

1400 Eye Street, NW, Suite 450
Washington, DC 20005
fpf.org