SPECIAL REPORT

DECODING GENOMIC DATA SECURITY:

LESSONS FROM FTC'S VITAGENE ENFORCEMENT AND THE NIST CSF PROFILE FOR GENOMIC DATA

AUGUST 2023

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

LEARN MORE

For more information, please contact your regular McDermott lawyer, or:

JENNIFER S. GEETTER
PARTNER

jgeetter@mwe.com
Tel +1 202 756 8205

SAM SIEGFRIED
ASSOCIATE

ssiegfried@mwe.com
Tel +1 312 803 7017

ALYA SULAIMAN
PARTNER

asulaiman@mwe.com
Tel +1 310 788 6017

For more information about McDermott Will & Emery visit mwe.com

INTRODUCTION

Remarkable progress in DNA and RNA sequencing have democratized the generation and analysis of genomic data across diverse industry sectors, including biopharmaceutical research, healthcare, consumer ancestry, law enforcement, agriculture and wellness testing. However, these advances have simultaneously escalated cybersecurity risks associated with the collection, processing, and maintenance of genomic data. This burgeoning challenge has prompted state attorneys general and federal agencies to take action to safeguard consumers and ensure responsible genomic data management. Here we examine recent state and federal enforcement actions and guidance from the National Institute of Standards and Technology (NIST) that address the responsible collection, storage and use of genomic data. We summarize key issues and recommendations to help genomic community stakeholders manage and reduce cybersecurity risks.

BACKGROUND

Recent advances in high-throughput next-generation DNA and RNA sequencing have made generating and analyzing genomic data more accessible and affordable. These advances have catalyzed the growth of a diverse genomics community that spans several industries, including biopharmaceutical research, healthcare, consumer ancestry, law enforcement, agriculture, and wellness and health testing. While increased availability of human and other genomic data promotes scientific and medical discoveries, it also creates new and challenging cybersecurity risks for organizations that generate, analyze and maintain genomic data. As a result, state attorneys general and federal agencies have recently initiated enforcement actions and issued guidance to protect consumers and promote the responsible collection and storage of genomic data.

For example, at the state level, attorneys general of Pennsylvania and Ohio entered into a multistate settlement with DNA Diagnostic Centers, Inc (DDC), a consumer genetic testing laboratory that offers diagnostic and genetic tests directly to consumers in the context of fertility and general health and wellness. The enforcement action resulted from a breach of Social Security numbers and other information of DDC consumers and included concerns that DDC received repeated warnings of vulnerabilities to its data systems but did not promptly investigate and remediate the issues.

One notable component of this enforcement action was that the breach principally involved data from a business unit that DDC acquired; the security vulnerabilities were present in the acquired company's systems. This underscores the need for companies that are growing by acquisition to (1) carefully assess the security controls of legacy information systems and (2) perform a comprehensive data inventory to determine whether appropriate controls have been applied and legitimate business needs exist for the data they are acquiring (especially given the implicit value of data in many of these transactions).

At the federal level, on June 16, 2023, the Federal Trade Commission (FTC) announced a first-of-its-kind enforcement action against a consumer genetic testing company, 1Health.io Inc. (formerly known as Vitagene, Inc., or Vitagene), alleging unfair and deceptive trade practices with respect to 1Health's genetic information privacy and security practices (the Vitagene action).

Also in June, the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) released its draft Cybersecurity Framework Profile for Genomic Data (CSF Profile for Genomic Data, or CSF Profile), which outlines voluntary, proactive guidance to help organizations manage cybersecurity risks for systems that process genomic data.

We discuss the Vitagene action and the NIST CSF Profile for Genomic Data in detail below.

It is important to note that neither of these developments sought to change the status quo as to characterizing the identifiability of genetic or genomic information or related re-identification risks. Genetic and genomic information, absent being linked with or containing other identifiable information or metadata, can still be considered de-identified health information.

FTC VITAGENE ACTION

On June 16, 2023, the FTC published a proposed complaint and proposed settlement and order against Vitagene, a company that markets DNA test kits and health reports to consumers. For one type of health report, Vitagene contracts with a lab to analyze a saliva sample provided by the consumer and combines the resulting DNA analysis with the consumer's answers to an online health questionnaire to generate reports about the consumer's health, wellness and ancestry. Vitagene

also markets a second type of health report to consumers that it creates by combining a consumer's answers to an online "lifestyle questionnaire" with raw DNA data that the consumer obtains from certain other DNA testing companies and submits to Vitagene. Vitagene stores consumers' health and genetic information in cloud-based servers using virtual containers called "buckets."

In its enforcement action, the FTC alleges Vitagene misled consumers about data security standards they could expect from the company (for example, by claiming to be "HIPAA compliant" even when such companies were not subject to HIPAA). In this respect, the Vitagene enforcement action is of a piece with other FTC actions and guidance that have raised concerns about companies overstating their data security sophistication, thereby giving consumers a false sense of confidence in entrusting sensitive information to such companies. The proposed five-count complaint alleges Vitagene violated Section 5(a) of the FTC Act by misrepresenting the company's data security and privacy practices and by unfairly making material, retroactive changes to the company's policies regarding third-party sharing of sensitive personal information.

The first three counts of the proposed complaint allege Vitagene deceived consumers by misrepresenting that it (1) exceeded industry-standard security practices by claiming on its website that it "use[s] the latest technology and exceed[s] industry-standard security practices to protect your privacy," (2) stored consumers' DNA results without name or any other common identifying information, and (3) would remove all of a consumer's information if the consumer requested deletion of their data.

Despite these assertions, the proposed complaint alleges that in or about 2016 and continuing until July 2019, Vitagene stored health reports for at least 2,383 consumers and raw genetic data (sometimes accompanied by first name) for at least 227 consumers in publicly available buckets and failed to implement access controls to restrict access to this sensitive data, encrypt it, log or monitor access to it, or inventory it. According to the proposed complaint, Vitagene received at least three warnings between July 2017 and June 2019 that it was storing consumers' unencrypted health, genetic and other personal information in publicly accessible buckets. In addition, the proposed complaint alleges Vitagene's lack of a data inventory made it impossible for the company to honor consumers' data deletion requests, as Vitagene lacked a comprehensive mechanism to search and identify all instances of a consumer's data within the buckets.

The fourth count of the proposed complaint alleges Vitagene deceived consumers by claiming on its website that it destroys consumers' saliva samples shortly after sample analysis. The proposed complaint alleges that Vitagene did not have a contract provision with its genotyping laboratory partner requiring such destruction.

Finally, the fifth count of the proposed complaint alleges that Vitagene unfairly posted revised privacy policies on its websites in April and December 2020 that describe materially expanded practices for the company's sharing of consumers' sensitive health and genetic information with third parties, including consumer data that was collected before April 2020, without taking any additional steps to notify consumers or obtain consumers' consent.

Vitagene agreed to settle with the FTC without admitting liability. Under the terms of the proposed settlement, Vitagene is, among other things:

- Prohibited from misrepresenting (1) the extent to which it meets or exceeds industry-standard

security or privacy practices, (2) the extent to which it stores any health information with any other element of personal information, (3) the extent to which, or the purposes for which, it collects, uses, discloses, maintains, deletes or destroys a consumer's (i) physical DNA sample or (ii) personal information upon request, (4) that it is a member of, adheres to, complies with, is certified by or otherwise participates in any privacy or security program sponsored by a government entity or third party, (5) the extent to which it otherwise protects the privacy, security, availability, confidentiality or integrity of personal information, or (6) that it has received approval or authorization for its claims, products or services from any government agency.

- Prohibited from disclosing health information to any third party (as defined in the order) without the affirmative express consent of the individual who is identifiable by the health information.
- Required to instruct any laboratory that collected physical DNA samples pursuant to a contract with Vitagene to destroy any such sample that the laboratory retained for more than 180 days after Vitagene accepted the results of the sample analysis.
- Required to establish, implement and maintain a comprehensive information security program that protects the security, confidentiality and integrity of personal information.
- Required to obtain initial and biennial data security assessments from a third-party assessor for 20 years and to disclose, and not misrepresent, all material facts to the assessor.
- Required to submit to an annual certification to the FTC that it has implemented the requirements of the order and is not aware of any material noncompliance that has not been corrected or disclosed to the FTC.
- Required to submit a report to the FTC if it is required to issue breach notifications under applicable law or if it discovers other unauthorized use or disclosure of consumer health information.
- Required to pay $75,000 in monetary relief.

The proposed order, if approved, states that it will remain in effect for 20 years, with certain exceptions.

The Vitagene action is the latest of many reminders[1] this year that the FTC is actively pursuing enforcement related to privacy and security practices, as well as promises made to consumers, that the commission perceives to be deceptive, misleading or unfair, all with a particular focus on health information. All genomic data companies, and direct-to-consumer genetic testing providers, in particular, should take a close look at the privacy and security commitments they make to consumers and the public, and confirm that they and the entities they contract with have sufficient internal processes and controls to meet those commitments. In addition, companies should consider, where appropriate, obtaining consent from individuals for uses or disclosures of genomic data that are either new or would otherwise be contrary to consumer expectations.

NIST CSF PROFILE FOR GENOMIC DATA

Although the alleged information security lapses in the Vitagene action relate to controls that are common to information security programs across all industries, the

[1] FTC and HHS-OCR Spotlight Use of Tracking Tech by Healthcare Providers; FTC Proposes Health Breach Notification Rule Amendments

federal government is actively engaging with industry stakeholders to offer guidance to the genomics community more broadly to promote information security safeguards that address the unique challenges associated with genomic data.

In June 2023, the NIST released its draft Cybersecurity Framework Profile for Genomic Data[2] , which identifies 12 "Mission Objectives" and provides voluntary guidance to help organizations prioritize each of the 108 Cybersecurity Framework subcategories based on the Mission Objectives throughout the data lifecycle. The CSF Profile for Genomic Data was informed by public workshops and subgroups of stakeholders across industry, academia and government. The CSF Profile is a companion document to NIST's earlier publication, NIST Internal Report (NISTIR) 8432, The Cybersecurity of Genomic Data.

While the CSF Profile for Genomic Data focuses on cybersecurity risk, privacy is referenced in multiple places throughout the CSF Profile where cybersecurity and privacy risks overlap. NIST indicates it plans to offer separate guidance on managing privacy risks related to human genomic data by creating a profile for human genomic data based on the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management. NIST intends for that profile, once developed, to be used as a complementary tool to the CSF Profile for Genomic Data. Organizations may also find that elements of these profiles are useful for other forms of sensitive health information as well.

NIST notes that the CSF Profile is intended to supplement, not replace, current cybersecurity standards, regulations and industry guidelines applicable to health information. Organizations should consider their unique obligations, operating environments and community expectations when prioritizing and implementing the Mission Objectives and relevant cybersecurity controls.

Following is an overview of each Mission Objective from the CSF Profile:

- **Objective 1: Manage provenance and data integrity throughout the genomic data lifecycle**. Data provenance and integrity considerations impact all 12 Mission Objectives. Data provenance relates to the source and processing of the genetic information. Data integrity relates to an organization's ability to assure that data are correct and that the chain of provenance remains intact. NIST advises that organizations should implement cybersecurity controls that promote effective data storage and analysis and secure dissemination and sharing of data sets through interconnected systems.
- **Objective 2: Preserve privacy of relatives**. The commonality of genomic data among deceased, living and future biological relatives can reveal health conditions, disease histories and unknown relations and permit discrimination of identifiable populations. NIST advises that organizations

[2] A Cybersecurity Framework "profile" identifies and prioritizes opportunities for improving cybersecurity at an organization within a specific industry or sector based on a customized alignment of organizational requirements, objectives, risk appetite and resources against the desired outcomes of the "CSF Core." The CSF Core is an industry-agnostic catalog of desired cybersecurity activities and outcomes developed by NIST using common language that is easy to understand regardless of cybersecurity expertise. The CSF Core guides organizations in generally managing and reducing cybersecurity risks to complement existing cybersecurity and risk management processes.
Profiles serve as a useful starting point for identifying important cybersecurity activities and outcomes and can be used to identify opportunities to improve cybersecurity posture by comparing a "current" profile (the as-is state) with a "target" profile (the to-be state). Profiles also give organizations a consistent way to discuss cybersecurity objectives across organizational roles using shared terminology.

should identify where privacy risks to relatives may arise because of the organization's role in the genomic data processing ecosystem as well as in their internal operations.

- **Objective 3: Identify, model and address security and privacy risks to genomic data**. NIST advises that the ability to identify evolving cybersecurity threats or vulnerabilities to genomic data, and their associated potential impact if realized, is critical to selecting appropriate cybersecurity practices and ensuring that they address emerging capabilities that introduce new risks over time.
- **Objective 4: Manage informed consent throughout the genomic data lifecycle**. In addition to privacy processes, cybersecurity plays a role in ensuring data processing activities are consistent with informed consent through appropriate access controls and data protection mechanisms. NIST advises that procedures to review consent if and as needed should be established to ensure the operational environment and any applicable consents obtained from genomic data subjects remain in sync over time. Notably—and in deference to applicable law—this standard does not establish when consent is required. Rather, it focuses on establishing controls for revising consent requirements, such as when data processing practices and purposes of use change.
- **Objective 5: Preserve privacy of donors**. Processing human genomic data presents unique privacy challenges throughout the data processing lifecycle. NIST advises that appropriate cybersecurity safeguards help protect against loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of genomic data.
- **Objective 6: Manage authorized data access**. An organization's ability to grant access to authorized users and prevent unauthorized usage enables other Mission Objectives. NIST advises that organizations should establish appropriate data access controls to manage who can access data, who has authority to grant access, and what permissions can be granted. These permissions should be modifiable or revokable in alignment with donor consent permissions.
- **Objective 7: Maintain trust and manage reputational risk**. Failure to maintain trust and manage reputational risk could put other Mission Objectives at risk. NIST advises that organizations can build and maintain the trust of genomic data subjects through responsible and effective genomic data management, privacy and security practices (such as network monitoring, threat detection process improvements, consistent application of incident response and mitigation practices, and training regarding reputational risks of genomic data breaches) along with the legal and regulatory compliance described in other Mission Objectives.
- **Objective 8: Facilitate research and education to advance science and technology**. NIST advises that ensuring clear communication and understanding between scientific and cybersecurity professionals for safe storage and management of genomic data can prevent potential data loss and disruptions to research and education focused on realizing the full potential of genomic data. In addition, maintaining the integrity and availability of the research environment through cybersecurity controls can also help ensure the reproducibility of a study.
- **Objective 9: Maintain compliance to laws and regulations**. Organizations processing genomic

data face unique challenges that require stricter compliance with national and international laws and regulations. NIST advises that organizations should ensure their cybersecurity activities support compliance with applicable laws, regulations, Good Practices (GxP) and other standards of practice.

- **Objective 10: Protect intellectual property**. Many organizations working with genomic data develop intellectual property, such as trade secrets or patentable information. In some cases, operations require indefinitely sequestering genomic information and associated analyses until they can be shared or disclosed. NIST advises that these organizations implement cybersecurity controls designed to protect these assets and associated business interests.
- **Objective 11: Enable and preserve sample diversity**. Sample diversity allows organizations to access genetic variants that contribute to a more comprehensive and inclusive understanding of diverse populations and reduce privacy risk. While many activities related to sample diversity occur before genomic data collection, NIST advises that organizations should implement cybersecurity controls designed to promote the data provenance and integrity of genomic data, to help inform and track sample collection in order to promote biorepositories that have an inventory from diverse populations.
- **Objective 12: Promote the use of secure platforms for the controlled sharing of genomic data**. Many organizations working with genomic data prefer to bring people to the data rather than share data across multiple environments. NIST advises organizations to consider implementing secure platforms that provide the ability to (1) enforce consistent security practices, (2) manage provenance, (3) ensure data integrity, (4) restrict access to authorized entities and (5) enhance incident/breach response, all while promoting the safe and controlled use of the genomic data. A secure platform may take many forms and use a range of components provided by multiple organizations. NIST emphasizes that organizations should consider the resilience of these platforms and evaluate how third-party platform providers integrate appropriate cybersecurity and privacy risk management practices.

CONCLUSION

Genomic data has been a significant driver of recent advances in biotech and innovation, including vaccine development, pharmaceutical development, disease diagnosis, agricultural innovations, basic and translational scientific research, consumer genetic testing, genealogy and law enforcement. As the DDC and Vitagene settlements demonstrate, in many ways genetic and genomic data are vulnerable to the same pitfalls as other types of health data. The same challenges that have confronted other consumer health markets can also frustrate public trust in consumer genetic testing and genomic sequencing, so careful attention should be paid to public assurances about privacy and security.

At the same time, genomic data are not just the same as other types of health data, and the new NIST CSF Profile for Genomic Data provides examples of how to build a genomic-specific standard for articulating and addressing the particular privacy and security concerns surrounding the collection, storage and use of genomic data. As the volume of genetic and genomic information grows, it is important for consumer genetic testing providers, clinical genomic sequencing labs, biopharma companies and other

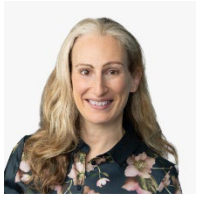
organizations that use, analyze and store genomic data to:

- Align their privacy and security programs with current guidance on industry best practices.
- Incorporate learnings from FTC enforcement actions against similar companies.
- Build cybersecurity programs designed for sensitive data and future threats.

If you have questions or want to learn more, please contact any of the authors or your regular McDermott lawyer.

.

CONTRIBUTORS



JENNIFER S. GEETTER
PARTNER
jgeetter@mwe.com
Tel +1 202 756 8205

SAM SIEGFRIED
ASSOCIATE
ssiegfried@mwe.com
Tel +1 312 803 7017

ALYA SULAIMAN
PARTNER
asulaiman@mwe.com
Tel +1 310 788 6017

McDermott
Will & Emery

mwe.com |