Privacy Implications for Biotechnology

by Patricia Wagner

As biotechnology companies continue to grow and develop new business models, including models that have more direct interaction with consumers, there are a number of privacy-related laws and regulations of which the companies should be aware. Different products can trigger different requirements. This article provides an overview of the privacy and security framework in the United States.[1] Ultimately, the concern of state and federal regulators is that individuals' privacy rights are protected, and that individuals have fair and adequate notice of how their information will be used, stored and disclosed. The discussion below provides a high-level description of the various privacy regimes.

The Federal Trade Commission

The Federal Trade Commission (FTC) has jurisdiction over companies, including biotechnology companies, operating in the United States. In the privacy realm, a biotechnology company could come under the purview of the FTC if it collects information from consumers in any way. The collection could take place from a company website (even, for example, a mere request for additional information), from a device, from a smartphone application (an app) or from other sources. The FTC has been increasingly active in investigating organizations that collect, but (allegedly) fail to appropriately protect consumer information.[2] In addition, the FTC has made it clear that even those entities that are subject to regulation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[3] are still subject to the FTC's jurisdiction.[4]

The FTC asserts its jurisdiction under the Federal Trade Commission Act,[5] which prohibits "unfair or deceptive acts or unfair practices in or affecting commerce.[6] In bringing actions against organizations related to privacy issues, the FTC is likely to allege that failures to adequately describe the data collection processes are "deceptive acts or unfair practices prohibited by

Biotechnology companies can mitigate the risk of privacy concerns by including privacy in the initial design of products and consumer outreach....[C]ompanies should take steps to understand how the technology will work in the consumer space or healthcare space, as well as what information the company will want to collect from consumers, and attempt to understand how that may change in the future.

Section 5(a) of the FTC Act."[7] The Federal Trade Commission Act defines "unfair practices" as those "that [cause] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[8]

The FTC's active enforcement in the privacy space can relate to a company's representations in its website or app privacy notices, or other representations made by the company. If the FTC staff suspect (usually from receiving a complaint from a consumer) that an organization is using information in a manner not adequately described in the organization's information, the staff can open an investigation. In such a case, FTC allegations can lead to a consent order issued by the FTC, which requires active monitoring and reporting to the FTC. In addition, in the event of consumer financial harm, the FTC can bring an action under Section 13(b) of the Federal Trade Commission Act, and seek monetary restitution for consumers.[9]

HIPAA Considerations

In addition to the Federal Trade Commission Act, those biotechnology companies in the healthcare space may also have to address concerns related to HIPAA. HIPAA, and its implementing regulations, established the federal criteria regarding: 1) the maintenance of privacy and confidentiality of individually identifiable health information (the privacy rule); 2) the notification in the event of a breach of that health information (the breach notification rule); and 3) the security of electronic health information (the security rule).[10]

HIPAA and its implementing regulations apply only to covered entities (such as health plans, healthcare providers, and healthcare clearinghouses) and the business associates of those covered entities. Business associates are vendors that are performing a task on behalf of a covered entity. Both covered entities and business associates must meet a number of requirements under the privacy and security rules.[11] For example, both covered entities and business associates are required to perform a risk analysis to identify where electronic health information is stored, the protections for the security and integrity of that information, and mitigation steps taken to protect the information. Similarly, both covered entities and business associates must contractually bind vendors to protect health information being accessed or created by the vendor.[12]

Failure to meet the requirements of the privacy and security rules can result in significant penalties. Under HIPAA, the penalties for a violation of the requirements can range from $100 for each violation up to $50,000 for each violation, with a maximum for all violations of an identical provision in a calendar year of $1.5 million.[13] The Department of Health and Human Services Office for Civil Rights (OCR), the agency charged with enforcing the privacy and security rules, has made it clear that violations can be cumulative. For example, the breach of health information could result in a fine for the impermissible use or disclosure (*e.g.,* the loss of the information), as well as a failure to develop appropriate safeguards to protect the information, resulting in possible penalties in excess of $1.5 million.[14]

OCR has instituted an audit program to evaluate the privacy and security compliance of both covered entities and business associates.[15] In addition, OCR has opened investigations related to reported breaches or other consumer complaints.[16]

FDA Considerations

The Food and Drug Administration (FDA) has also been monitoring privacy of medical devices.[17] To further the goal of ensuring that patients' information is adequately protected, on Jan. 12, 2017, the FDA held a webinar on the cybersecurity of medical devices. The FDA also issued guidance in late 2016. That guidance provided recommendations for management of cybersecurity vulnerabilities, and recommends that organizations "monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices."[18]

State Privacy Laws

In addition to the federal regimes, there are a number of state privacy laws that increasingly apply to organizations. The majority of states have now enacted state laws requiring companies that collect and/or store personal identifying information (such as Social Security numbers, driver's license numbers, and credit card numbers) to notify consumers if there is a loss of that personal identifying information.[19] In addition, some states have taken additional steps

to ensure that such information is protected. As drafted, these state laws would reach any company storing information related to citizens of that state. For example, Massachusetts has enacted a law that requires any company storing personal identifying information provide appropriate security measures to protect that information, train employees on how to handle and protect that information, and notify individuals if that information is compromised.[20] Similarly, Texas has enacted a state law that requires any entity (not just covered entities as defined under the federal privacy rule) that comes into contact with health information to provide, among other things, training for employees on an ongoing basis. The Texas law also provides for civil penalties, ranging from $5,000 to $1.5 million, for entities that wrongfully disclose an individual's health information.[21]

In addition, many states have enacted statutes that dictate the processes for genetic testing and the collection of information related to that testing.[22] Those states always allow the consumer to authorize such collection and analysis; however, the statutes dictate the parameters of disclosure beyond the requesting consumer (for example, requiring explicit authorization before the genetic information could be shared with a payor). In addition, some states have statutes that specifically provide privacy protections for DNA samples, as well as providing that the DNA samples and results of those samples are the exclusive property of the person sampled or analyzed.[23] In addition to enforcing state privacy laws, states attorneys general can enforce privacy requirements through the Unfair Trade Practice Act, much like the FTC, and have the authority to enforce HIPAA.

Mitigation Steps

Biotechnology companies can mitigate the risk of privacy concerns by including privacy in the initial design of products and consumer outreach. During the development process, companies should take steps to understand how the technology will work in the consumer space or healthcare space, as well as what information the company will want to collect from consumers, and attempt to understand how that may change in the future. Similarly, companies should ensure that any website or app privacy statement accurately reflects how the company will collect information, what it will do with information, who else will have access to the information, and how it will take steps to ensure the information is secured. A company should also periodically review its privacy statement to ensure it has been modified as data collection and/or usage changes. ⚖

Patricia Wagner *is a member of Epstein Becker & Green's healthcare and life sciences and litigation practice groups, in the firm's Washington, DC, office. Wagner regularly advises clients on a variety of matters related to federal and state privacy issues. She also serves as the chief privacy officer for the firm.*

ENDNOTES

1. Those biotechnology companies that are operating outside of the United States will have additional obligations from the appropriate jurisdiction.
2. For a listing of such actions, *see*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.
3. Health Insurance Portability and Accountability Act, Subtitle F, Public Law 104-191. The implementing regulations can be found at 45 C.F.R. Parts 160, 162 and 164.
4. For example, see the FTC's action against a laboratory testing company at https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.
5. 15 U.S.C. § 45(a).
6. 15 U.S.C. § 45(a).
7. 15 U.S.C. § 45(n); *see,* for example, *In re PaymentsMD, LLC,* Docket No. C-4505, *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.
8. 15 U.S.C. § 45(n).
9. 15 U.S.C. § 53(b).
10. Health Insurance Portability and Accountability Act, Subtitle F, Public Law 104-191. The implementing regulations can be found at 45 C.F.R. Parts 160, 162 and 164.
11. Covered entities also have to afford individuals certain rights to access information under the privacy rule, and provide individuals with a notice of privacy practices that describes how the covered entity and its vendors will use and disclose the individuals information. For example, *see*, 45 C.F.R. §§164.520, 164.524, 164.526, and 164.528.
12. *See* 45 C.F.R. §§164.308, and 164.504. For a full list of privacy and security rule requirements *see* https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/ and https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/.
13. 45 C.F.R. §160.404.
14. 78 Fed. Reg. 5566, 5584 (Jan. 25, 2013).
15. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html?language=es.
16. http://www.hipaajournal.com/ocr-to-increase-investigations-of-small-phi-breaches-3558/.
17. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.
18. *Postmarket Management of Cybersecurity in Medical Devices,* available at https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm.
19. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
20. *See* M.G.L. c. 93H, M.G.L. c.93I, and 201 CMR 17.00 *et. seq*.
21. Tex. Health & Safety Code §181.001.
22. https://www.healthlawyers.org/hlresources/Public%20Documents/50state_chart_final.pdf.
23. *See e.g.,* AK Stat. §18.13.010 *et. seq*.