Stay Current

PAUL HASTINGS

August 2025

Follow us on LinkedIn

Litigation Update

At the Crossroads: Illumina Settlement Reflects Intersection of Cybersecurity and Healthcare Law

By Gary F. Giampetruzzi, Wendy Goldstein and Jack Hibbard

On July 31, the U.S. Department of Justice (DOJ) announced a settlement in *United States ex rel. Lenore v. Illumina, Inc*, the first case in which underlying cybersecurity issues formed the basis of a settlement under the False Claims Act against a healthcare products producer.

Illumina, a biotechnology firm based in California, agreed to pay $9.8 million plus 4.33% interest to resolve alleged False Claims Act violations, with $1.9 million designated for the relator. The settlement was based on allegations that Illumina knowingly misrepresented the strength of its cybersecurity protections in connection with the sale of several of the company's genomic sequencing systems to federal agencies including the DOJ, the Department of Health and Human Services, the Department of Veterans Affairs, NASA, and the Army, Navy and Air Force, between February 24, 2016, and September 28, 2023.

The underlying qui tam complaint, filed by Erica Lenore, a former director for Platform Management at Illumina, focused on three alleged cybersecurity defects: (i) Illumina elevated privileges to everyday users, giving them enhanced visibility into sensitive information; (ii) Illumina failed to protect user credentials by "hard-coding" products and not requiring authentication / encryption; and (iii) it failed to mitigate risks from insiders, for example, by taking minimal efforts to shield confidential information from hacks by Illumina employees. Illumina denied the allegations.

Expanding the DOJ's Civil Cyber-Fraud Initiative to Healthcare Products

The compliance and defense bars in the life sciences and healthcare sectors were waiting for this case to come along. In October 2021, then-Deputy Attorney General Lisa Monaco announced the launch of the Civil Cyber-Fraud Initiative, explaining that the DOJ would "use [its] civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards[.]"

Since then, the DOJ pursued several cases against companies for failure to maintain adequate cybersecurity safeguards. Notably, the first of these cases was against a healthcare provider, Comprehensive Health Services (CHS). The government alleged that CHS had agreed to provide medical support services at government facilities in Iraq and Afghanistan. While CHS had submitted claims suggesting it had uploaded medical records onto a secure electronic medical record system, it had in fact scanned patient records and left them on an internal network drive that was accessible to non-clinical staff.

However, *Illumina* is the first case under the Cyber-Fraud Initiative against a healthcare company selling products. The *Illumina* resolution suggests that the intersection of cybersecurity and healthcare fraud enforcement is here.

The DOJ intervened in the underlying qui tam suit and, in the settlement, alleged that Illumina submitted, or caused to be submitted, false claims for its genomic sequencing systems. Specifically, the government alleged that Illumina knowingly failed to build cybersecurity into its software design, failed to adequately resource its product security functions, failed to correct design features that exposed certain cybersecurity vulnerabilities and falsely represented that the software its products used adhered to applicable Food and Drug Administration (FDA) cybersecurity guidelines.

The FDA's Quality System regulation, or QSR (see 21 C.F.R. § 820 et seq.) applies to medical devices and requires manufacturers to create procedures to ensure compliance with particular design requirements and to implement means of addressing quality problems (both reactively and proactively). It also requires that senior management at device manufacturers be involved in implementing and socializing quality policies. Under the government's theory, Illumina failed to satisfy these requirements and misrepresented such failures in certifying compliance with FDA cybersecurity guidelines. According to the DOJ, Illumina sought payment directly from the government either in connection with government grants or contracts, or indirectly from grants issued to third parties for the purchase of Illumina products. The DOJ claimed that such payments would not have been made absent the FDA certification described above. Significantly, the government argued that the claims were false *regardless* of whether any cybersecurity breach in fact occurred.

Implications for Life Sciences Companies

The *Illumina* resolution suggests potential widespread implications from the enforcement of cybersecurity regulations for software as a medical device and software in a medical device, even absent the occurrence of a data breach. Life sciences and healthcare companies should take formal and systemic steps to assess cyber risk areas and evaluate their data privacy and security compliance programs. Such action not only mitigates the company's risk of a cybersecurity attack or data breach but also reduces the chance of QSR non-compliance. This precaution is especially important for emerging companies in the digital health space that are new to healthcare regulatory and compliance requirements.

Finally, companies operating in this space should consider third-party compliance reviews and gap assessments to ensure compliance with relevant laws and certifications. Obtaining an outsider's view on a company's cybersecurity operations can help validate current measures, identify room for improvement and provide evidence of the good-faith attempts to ensure compliance.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings New York lawyers:

Gary F. Giampetruzzi
+1-212-318-6417
garygiampetruzzi@paulhastings.com

Wendy Goldstein
+1-212-318-6411
wendygoldstein@paulhastings.com