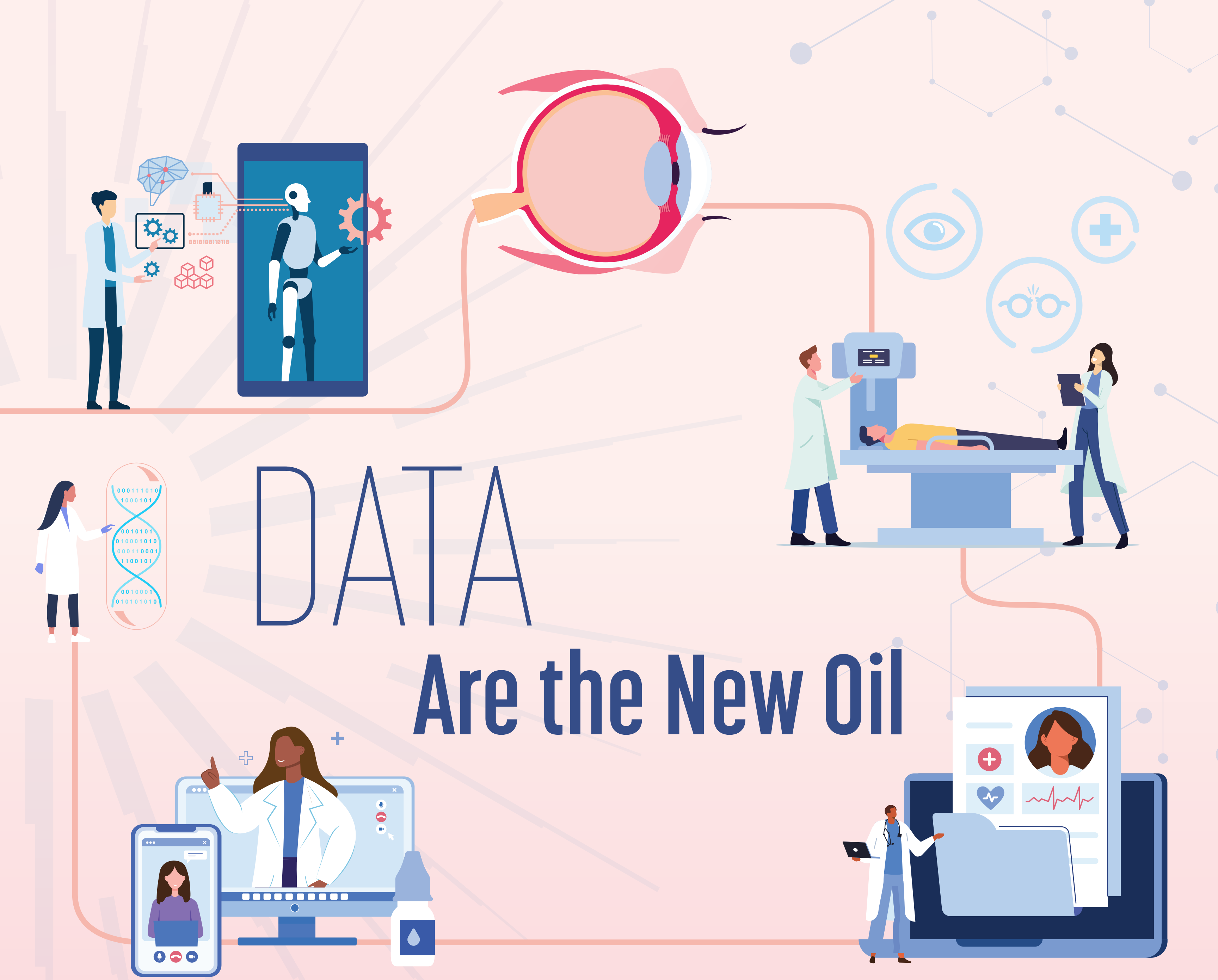

DATA Are the New Oil

BY LAURA STRAUB, EDITOR-IN-CHIEF

> Privacy and security must be maintained.

IBM defines *data sovereignty* as “data being subject to the laws and governance structures from within the jurisdiction where it is generated or collected.”[1] Data sovereignty is closely related to data security, cloud computing, and network and technological sovereignty. The concern, however, is the data itself.[2]

More than 100 countries have their own unique data sovereignty laws that regulate the control and storage of data in their country.[3] These laws affect how an individual, organization, or government can collect, process, store, and transfer data. Data sovereignty laws are complex, but the reigning principle is simple: Individuals and organizations should have control over their own data. I recently sat down with Lama A. Al-Aswad, MD, PhD, to discuss the importance of data sovereignty in ophthalmology. This article reviews some of the topics we covered during our conversation.

HOW DATA SOVEREIGNTY PERTAINS TO OPHTHALMOLOGY

Advances in technology, the increased use of digital devices, and the incorporation of big data and AI have helped ophthalmologists make more accurate diagnoses, customize patient care, and achieve better patient outcomes. The introduction of cloud computing, electronic health records, and data sharing and management has also given rise to concerns about patient privacy, confidentiality, security, and legal and regulatory compliance. Laws and regulations are trying to catch up with the boom in technology. The biggest questions today are who owns data, and how are data accessed and protected?

Ophthalmologists gather a lot of data from patients, including their medical records, diagnostic tests and images, genetic information, treatment plans, and postoperative follow-up measurements. Patient privacy must be protected and their data safeguarded according to the laws of the region where they are collected, whether that be at a state, federal, or national level.

Like most data centers, the data center at NYU Langone, where Dr. Al-Aswad practices, enforces stop gaps to maintain data sovereignty and security. Data are deidentified and anonymized and made accessible only to authorized individuals on a full or granular level, Dr. Al-Aswad explained. Additionally, patients have a say in how their data are shared, and they have the right to revoke access to or request deletion of their data. This helps patients maintain their privacy and increases their confidence in NYU Langone's health care system and providers.

ESTABLISHING TRUST

Upholding data sovereignty helps establish trust and accountability with patients. In the past, patients did not think too much about who could share or see their data. That has changed in the digital age. Now, patients want to protect their data. The Health Insurance Portability and Accountability Act (better known as HIPAA) has empowered individuals to take a more active role in managing their health data through patient portals, mobile apps, and even wearable health-monitoring devices. It also shifted the ownership and control of health data to the patient.

Both data sovereignty and data security are integral to patients' trust in the health care system. If they trust the system, they are more willing to share their data. Their trust is essential to moving toward an era of AI, precision medicine, and patient-centric care. The more data ophthalmologists have, the better they can understand diseases and treat each individual. (To learn more about precision medicine, read the article, "Back to the Future," pg 26.)

> "As technology continues to advance, it is crucial to strike a balance between leveraging the benefits of digital health data and guarding data sovereignty and individual privacy.

CONSIDERATIONS

Several issues must be addressed to protect data sovereignty and build patients' trust in ophthalmology.

Data storage. Ophthalmic data are generated by different devices and stored in multiple locations. The interoperability of systems and databases adds another layer of complexity. Seamless and secure data exchange must be ensured while data sovereignty is maintained.

Data breaches. Any breach in data security or unauthorized access to health data compromises patient privacy. Ophthalmologists' reliance on digital platforms and cloud storage solutions increases the risk of cybersecurity threats. Robust security measures such as encryption of data, rigorous access controls, and regular audits can help protect against data breaches.

Ethical considerations. The AI era is possible only because of the accumulation of data. Data accessibility, however, poses ethical considerations. Some data are old, and patients might not have agreed to share the information. Also, who owns data? Do we have the right to use data to train AI algorithms? These are crucial questions that people such as Dr. Al-Aswad are trying to answer. Those who want to learn more about the ethics of AI in medicine and ophthalmology may be interested in an article Dr. Al-Aswad and her colleagues published in the *Asia-Pacific Journal of Ophthalmology*.[4]

PROMOTING DATA SOVEREIGNTY

Ophthalmology practices should devise their own programs to help safeguard data sovereignty. Points to consider include the following:

- Data governance frameworks to outline policies, procedures, and responsibilities in data management;
- Proper informed consent that outlines how patient data will be collected, used, and shared;
- Secure infrastructure to protect data from unauthorized access;
- Data localization policies that ensure data are stored within the jurisdiction where they were collected; and
- Interoperability standards that encourage secure connections between different software systems and databases.

A data sovereignty program should address data collection, storage, sharing, consent, and security protocols. It should also comply with relevant local and national laws and regulations such as the Federal Trade Commission Act and the US Privacy Act of 1974 in the United States and the General Data Protection Regulation in Europe.

THE BOTTOM LINE

Digitalization has sparked a shift in people's attitudes toward health data and their management. The digital era has highlighted the importance of privacy, security, individual control, and responsible data management practices. As technology continues to advance, it is crucial to strike a balance between leveraging the benefits of digital health data and guarding data sovereignty and individual privacy. ■

1. Iyengar A. Data sovereignty at the edge. IBM. August 18, 2022. Accessed May 19, 2023. https://www.ibm.com/cloud/blog/data-sovereignty-at-the-edge
2. Irion K. Government cloud computing and national data sovereignty. *Policy & Internet*. 2012;4(3-4):40-71.
3. Gilmore D. DataFleets. Google scrapped cloud initiative in China, other markets. *Bloomberg News*. July 8, 2020. Accessed May 18, 2023. https://www.bloomberg.com/news/articles/2020-07-08/google-scrapped-cloud-initiative-in-china-sensitive-markets
4. Ibraheem AY, Schuman JS, Shabsigh R, Caplan A, Al-Aswad LA. Ethics of artificial intelligence in medicine and ophthalmology. *Asia-Pac J Ophthalmol*. 2021;10(3):289-298.

LAMA A. AL-ASWAD, MD, MPH

- CEO, Envision Health Technologies and Visi Health Technologies
- laa2003@cumc.columbia.edu
- Financial disclosure: Advisor (AI Optics, Carl Zeiss Meditec); Board member (Envision Health Technologies, Sensory Sciences, Visi Health Technologies); Consultant (Alcon, Americas Inc, Bausch + Lomb, iCare, World Care Clinical); Equity owner (GlobeChek); Grant support (Mother Cabrini Foundation, Save Vision Foundation); Research support (Topcon Medical Systems)