



## GUEST EDITORIAL

# Regulators must step in to safeguard patient data in the AI era



By **Mika Newton**  
CEO, xCures

The healthcare sector's necessary transition towards electronic health records (EHRs) has transformed patient care and operational efficiency.

While traditional regulation has focused on patient privacy and the security of their medical records, the patient's right of access to their data and the explosion of new AI technology have combined to create a new landscape for the digital management and exchange of medical records.

This shift, while offering opportunities for healthcare improvements, clinical trials, and other studies, raises ethical and privacy concerns that demand urgent regulatory attention.

Though these additional uses for healthcare data will advance medical science, it will also require regulatory frameworks to ensure patient privacy, ethical data use, and transparency. It is through the lens of these three pillars—

privacy, ethics, and transparency—that we must examine the necessity for oversight in the era of EHRs.

## Ensuring patient privacy in the digital age

Without doubt, EHRs provide significant benefits in terms of accessibility and efficiency, but their widespread adoption may also expose patient data to increased risks of unauthorized access and cyber threats.

The convenience of having medical records just a few clicks away comes with the downside of making sensitive information potentially accessible by hackers; convenience and security are antagonistic goals.

High-profile incidents of data breaches in healthcare institutions, affecting millions of patient records, highlight

the need for enhanced protection measures. These breaches not only compromise the privacy and security of personal health information but can also lead to identity theft and financial fraud.

The Health Insurance Portability and Accountability Act (HIPAA) in the United States serves as a critical foundation for patient privacy protection. However, the evolving nature of cyber threats and the complexities associated with managing digital records necessitate ongoing updates to HIPAA's provisions.

This means not only refining existing regulations to counteract new types of cyber attacks, but also introducing additional measures tailored to the digital age. These could include, for example, encryption standards, mandatory breach notification protocols, additional training for medical staff with access to PHI, and the integration of cybersecurity technologies within EHR systems.

## The imperative for ethical data use

The emerging use cases for health data hold immense promise for the future of medical innovation and the practice of healthcare. As these new use cases evolve, the potential for breakthroughs in understanding diseases, developing new treatments, and enhancing patient care is unparalleled.

Collaborations facilitated by the exchange of this data can accelerate scientific discovery and the development of targeted therapies that could improve patient outcomes on a global scale. However, it will be critical to remember the ethical implications of collecting, sharing, and using this data. Without ethical guidelines and careful oversight, the benefits of data sharing could be overshadowed by risks to patient privacy and autonomy.

One of the most pressing ethical concerns in the use of health data is the potential for exploitation and misuse. Anonymized data, if not protected, could be re-identified, which would compromise patient confidentiality and violate their rights.

Moreover, the trend towards the commercialization of health data raises questions about equity and consent: who benefits from the use of this data, and do patients have a say in how their information is used?

The risk of organizations prioritizing profit over public health benefits is an ethical dilemma and would erode trust in our healthcare system. We must ensure that data use is aligned with the principles of beneficence, justice, and respect.

Regulators, healthcare providers, and researchers must work together to establish protocols that prioritize patient welfare and public health outcomes over commercial gains. By doing so, the healthcare

sector can harness the power of health data to fuel scientific innovation and improve patient care, while also safeguarding the ethical principles and trust that underpin the doctor-patient relationship.

This includes frameworks to ensure transparency in data use, informed consent that respects patient autonomy, and robust data protection measures to prevent unauthorized access and re-identification.

## Upholding transparency in health data management

Transparency in the management, sharing, and use of patient data is necessary to uphold trust in the healthcare system. This includes specifics about data usage, the entities with which one's data is shared, and the purposes behind such exchanges.

Such a level of transparency will empower patients to make informed decisions about their care and about participating in initiatives that use their data for the advancement of clinical care.

Additionally, transparency serves as a catalyst for accountability among all stakeholders in the healthcare ecosystem, including providers, data handlers, and third-party entities involved in data analysis for both clinical care and research.

When healthcare organizations adopt transparent practices, we can expect it's more likely they'll conduct thorough assessments of their data management protocols, which will ensure they adhere to ethical standards and regulatory requirements. This culture of accountability is crucial for identifying and mitigating risks related to data privacy and security. It also encourages a proactive approach to safeguarding patient information and fosters an environment where ethical considerations are at the forefront of decision-making processes around data handling.

Finally, the commitment to data transparency and accountability could have a trickle-down effect that enhances the overall integrity of the healthcare system writ large.

By openly communicating how patient data is used and protected, healthcare organizations can build and maintain a strong bond of trust with the public, which is fundamental to the effective functioning of healthcare services and recruitment efforts for an increasing number of digital health initiatives that rely on access to a wide array of health data.

Ensuring that patients maintain control over their personal health information, and understand how it contributes to medical advancements, reinforces the ethical foundations of the medical system. Thus, the drive towards transparency in health data management is not just a regulatory requirement but a moral imperative to uphold the dignity and rights of patients.

## Next steps

The transition toward EHRs, while offering significant benefits for patient care and medical advancements, also brings to the forefront the need for comprehensive regulatory frameworks. Patient privacy, ethical data use, and transparency must be the guiding principles for navigating this digital transition.

It is only through the establishing robust regulations and oversight mechanisms that we can safeguard the interests of patients to ensure the digitization of health care serves the common good.

.....

*The author is the CEO of xCures, an AI-assisted platform that automatically retrieves and structures medical records from any U.S. care site. Newton holds over twenty five years of leadership experience in the life sciences.*