Yale University School of Medicine

Cite this as: *BMJ* 2023;381:p1225
http://dx.doi.org/10.1136/bmj.p1225
Published: 01 June 2023

In the US, patient data privacy is an illusion

Patients can no longer share personal information about themselves and be confident it remains private

Harlan M Krumholz *professor of medicine*

One of the sacred tenets of medicine is that our conversations with our patients are private. Those of us who have the privilege of being physicians walk into rooms where we engage strangers in intimate conversations that reveal sensitive details of their lives. People may share information they would not tell their closest friends or family. To be worthy of that trust, we learn to honour the special bond between doctor and patient, vowing never to violate their confidence.

However, the current digital transformation of medical data and the state of our federal US regulations threaten this trust. Patients can no longer share personal, stigmatising, or uncomfortable information about themselves and be confident that the conversation is truly private. Any words they utter now belong to the world of health information, which is expansive.

Today, the price of receiving healthcare is losing control of your private information. Medical privacy today is only an illusion. The digital transformation of medical data has opened many possibilities for improving healthcare, but has also led to the unconsented spread of sensitive information. This flow of information occurs among healthcare providers to whom you may not have originally disclosed the information, and private companies that work with health systems, or others to whom data are sold.

The US Health Insurance Portability and Accountability Act (HIPAA) is the federal law that protects sensitive patient information from being disclosed without the patient's knowledge or consent. The law seeks to protect the movement of health information to people not involved in a patient's care. However, the provisions of the law are permissive when it comes to organisations who have a relationship to a patient's care—whether that relationship is direct or tangential. Thus, there are pathways for data to move unencumbered to people who never received patient's permission to view, transmit, or commercialise that data.

The regulation allows anyone involved in a patient's care to access health information about them. It is based on the paternalistic assumption that for any healthcare provider or related associate to be able to provide care for a patient, unfettered access to all of that individual's health records is required, regardless of the patient's preference. This provision removes control from the patient's hands for choices that should be theirs alone to make. For example, the pop-up covid testing service you may have used can claim to be an entity involved in your care and gain access to your data. This access can be bought through many for-profit companies. The urgent care centre you visited for your bruised ankle can access all your data. The team conducting your prenatal testing is considered involved in your care and can access your records. Health insurance companies can obtain all the records. And these are just a few examples.

Moreover, health systems legally transmit sensitive information with partners, affiliates, and vendors through Business Associate Agreements. But patients may not want their sensitive information disseminated—they may not want all their identified data transmitted to a third party through contracts that enable those companies to sell their personal information if the data are de-identified. And importantly, with all the advances in data science, effectively de-identifying detailed health information is almost impossible.

HIPAA confers ample latitude to these third parties. As a result, companies make massive profits from the sale of data. Some companies claim to be able to provide comprehensive health information on more than 300 million Americans—most of the American public—for a price. These companies' business models are legal, yet most patients remain in the dark about what may be happening to their data.

However, massive accumulations of medical data do have the potential to produce insights into medical problems and accelerate progress towards better outcomes. And many uses of a patient's data, despite moving throughout the healthcare ecosystem without their knowledge, may nevertheless help advance new diagnostics and therapeutics. The critical questions surround the assumptions people should have about their health data and the disclosures that should be made before a patient speaks with a health professional. Should each person be notified before interacting with a healthcare provider about what may happen with the information they share or the data their tests reveal? Are there new technologies that could help patients regain control over their data?

Although no one would relish a return to paper records, that cumbersome system at least made it difficult for patients' data to be made into a commodity. The digital transformation of healthcare data has enabled wonderous breakthroughs—but at the cost of our privacy. And as computational power and more clever means of moving and organising data emerge, the likelihood of permission-based privacy will recede even further.

If we value privacy in medicine, we must use technologies that protect the content of sensitive

conversations, seek permission for sharing, and inform patients of the risk of disclosing sensitive information. People may worry about data breaches, but transmitting and selling their data as is routinely done may be a bigger threat. We should not assume that it is acceptable for people's secrets to become available to anyone connected with their care, including distant third parties.

The emerging belief in participation and partnership over paternalism has perhaps best been captured as "nothing about me without me." Now is the time to embrace this phrase by addressing the need to ensure patient privacy in medicine. If we are to maintain the ability to confide in our doctors—and know that our conversations will remain private—then such changes in our approach are essential. For the sacred trust between patients and their clinicians to survive, we must immediately promote strategies to give people more control.

Competing interests: In the past three years, Harlan Krumholz received expenses and/or personal fees from UnitedHealth, Element Science, Eyedentifeye, and F-Prime. He is a co-founder of Refactor Health and HugoHealth, and is associated with contracts, through Yale New Haven Hospital, from the Centers for Medicare and Medicaid Services and through Yale University from the Food and Drug Administration, Johnson and Johnson, Google, and Pfizer.

Provenance and peer review: not commissioned, not peer reviewed.