The State of Patient Privacy
Mental health startup Cerebral shared private patient data with Google, Meta and TikTok.

The company exposed the personal information of more than 3.1 million US users.

Congress presses Meta about health data privacy after hospitals remove Facebook tracker.

Hospitals pledge to protect patient privacy. Almost all their websites leak visitor data like a sieve.

With 385M patient records exposed, cybersecurity experts sound alarm on breach surge.

Cybersecurity experts say healthcare companies must harden their defenses, but it may require regulators and lawmakers to raise the bar on security standards.
Trust is the backbone of health information exchange.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Backdrop</td>
<td>5</td>
</tr>
<tr>
<td>Health Data Security</td>
<td>7</td>
</tr>
<tr>
<td>Data Exchange Purposes</td>
<td>14</td>
</tr>
<tr>
<td>Patient Access</td>
<td>21</td>
</tr>
<tr>
<td>Conclusion</td>
<td>28</td>
</tr>
</tbody>
</table>

**Health Data Security**
Patients are concerned about the security of their health data.

**Data Exchange Purposes**
Patients are nervous about use-cases beyond treatment.

**Patient Access**
Patients care a lot about medical record access.
Access to our medical records is opening up. We asked 1,213 patients how they feel about it.

Trust is the backbone of U.S. health information exchange: Trust in the platforms that store patient data, trust in the vendors that mediate exchange, and trust in the parties that access patient data. While the benefits of broader data sharing are well understood in the healthcare industry, the perspective of patients is rarely captured.

For this report, we surveyed 1,213 patients — with demographic and geographical distribution consistent with U.S. census data — to understand patient attitudes around health data exchange and the security and privacy of their medical information. Their responses provide us with never-seen-before insights into patients’ perceptions of the potential benefits and risk associated with sharing personal health information with third parties.

Why now?

Since the passage of the 21st Century Cures Act, more healthcare organizations are participating in national health information exchange than ever before. In February of this year, the U.S. Department of Health and Human Services (HHS) announced the first accepted Qualified Health Information Networks (QHINs), bringing the industry another step closer towards true nationwide interoperability. But as we push forward, we must confront the issues that prevent patients from being a confident participant. In this report, we set out to understand how patients are feeling about the evolving regulations around health data sharing, and what can be done to incorporate them into the national dialogue on data exchange.
Methodology

We surveyed 1,213 patients about their attitudes towards health information sharing. Age, gender, and geographic distribution were consistent with U.S. census data.
Patients are concerned about the security of their health data.
What best describes how you feel about a potential data breach or leak of your medical records?

- 28% Extremely concerned
- 42% Moderately concerned
- 25% Slightly concerned
- 5% Not concerned

An overwhelming majority of patients (95%) are concerned about a potential data breach or leak of medical records. Only 5% reported no concern at all.
54% of patients feel worried about whether companies handling health data are providing sufficient privacy and security protections.

Recent data breaches are difficult to forget.

In an era defined by technological advancements and digital connectivity, the healthcare industry has experienced a surge in data breaches, causing significant concerns regarding patient privacy and data security. Recent years have witnessed an alarming number of incidents where sensitive medical information has been compromised, leaving patients vulnerable to identity theft, fraud, and potential harm. Just in the last year, a number of high-profile healthcare companies — GoodRx, Cerebral, and BetterHelp among them — experienced data breaches, compromising the protected health information of millions of Americans.
Patients don’t trust Big Tech with their health data.

Why don’t people trust Big Tech with their health data?

In recent years, Big Tech companies have been embroiled in a number of controversies that include instances of unauthorized access, mishandling of user data, and an overall lack of transparency into data collection methods, all of which have eroded public confidence in their ability to properly safeguard health information.

Additionally, the business models of many tech companies, which rely heavily on data monetization, raise serious concerns about the commercialization of health information. Many patients fear that their health information is being exploited for targeted advertising or sold to third parties without consent.
A majority of patients (60%) feel more confident in health data exchange facilitated by government-approved entities.
What is the government’s role in health data exchange?

The federal government plays a significant role in health data exchange by establishing policies, regulations, and initiatives that promote interoperability and the secure exchange of health information. One key legislation in this domain is the 21st Century Cures Act, which was signed into law in December 2016. The act includes provisions aimed at accelerating medical product development, improving access to healthcare, and advancing health information technology.
The 21st Century Cures Act focuses on several aspects related to health data exchange:

1. Interoperability and Information Blocking
   The act addresses the issue of information blocking, which refers to practices that hinder or prevent the sharing of electronic health information. It establishes regulations to discourage information blocking and promotes the interoperable exchange of health information among healthcare providers, patients, and other authorized entities.

2. Trusted Exchange Framework and Common Agreement (TEFCA)
   The 21st Century Cures Act directs the Office of the National Coordinator for Health Information Technology (ONC) to develop a Trusted Exchange Framework and Common Agreement. TEFCA sets the groundwork for nationwide health information exchange by defining common technical standards, policies, and procedures for secure and interoperable data sharing.

3. Qualified Health Information Networks (QHINs)
   The act envisions the establishment of Qualified Health Information Networks, or QHINs, which are entities that meet certain criteria and are authorized to facilitate the exchange of health information at a national level. QHINs act as intermediaries between health information networks and provide the infrastructure and services necessary for secure data exchange.
Patients are nervous about use-cases beyond treatment.
A majority of patients (71%) are comfortable with sharing health data with healthcare providers for treatment purposes.

**What is the treatment use case?**

Health information can be exchanged for the purpose of providing medical treatment to an individual. This includes sharing relevant health records, test results, medication history, and other necessary information among healthcare providers involved in the patient's care. The primary goal is to support coordinated and effective healthcare delivery.
Only 39% of patients are comfortable with their health plans accessing their medical records.

**What is the payment use case?**

Payment refers to the authorized use and disclosure of individuals’ health information for activities related to billing, claims processing, reimbursement, and other financial transactions associated with healthcare services. It involves the sharing of relevant health data between healthcare providers, insurance companies, and other entities involved in the payment process.
Even fewer patients (28%) are comfortable with sharing their health data for operations purposes.

What is the operations use case?

Health information exchange may involve sharing data for administrative and operational purposes within healthcare organizations. This includes activities such as quality improvement, case management, billing, and internal audits. The exchange of information for operational purposes helps healthcare organizations function efficiently and provide high-quality care.
Government agencies accessing medical records for public health reasons? Fewer than a quarter approve.

**What is the public health use case?**

Health information exchange plays a crucial role in public health initiatives. It allows for the collection, analysis, and sharing of health data to monitor and respond to public health issues and outbreaks. This includes disease surveillance, epidemiological studies, and monitoring population health trends. Sharing health information for public health purposes helps identify and address health risks, track disease patterns, and facilitate timely interventions.
13% of patients are not willing to share their medical records for any reason.

Why are some patients opposed to sharing health data under any circumstance?

Some patients may be hesitant to share their health data, even for treatment purposes, due to concerns about privacy and security, lack of trust in the healthcare system, fear of stigma or discrimination, and a misunderstanding of how their data is used. Cultural and personal beliefs, as well as previous negative experiences, can also contribute to this reluctance. Building trust, ensuring transparency, and educating patients about the benefits and safeguards of data sharing are important steps in addressing these concerns.
De-identified data — data that is removed of personal identifiers, such as name, address, and date of birth — is a divisive topic.

While most patients (64%) are at least somewhat comfortable with their de-identified data being used for research purposes, 13% are extremely uncomfortable with their health data being used for research, even when it’s stripped of personal information.

De-identified data has a host of pros and cons.

**Pros**
- Honors patient privacy
- Allows for population research
- Enhances health policy and planning

**Cons**
- Runs the risk of re-identification (anonymized data is re-linked to the individual based on certain information)
- Potentially possesses limited utility for researchers

---

What best describes how you feel about companies that de-identify (removing personal identifiers such as name, address, and contact information) your medical records and extract insights for health/medical research purposes?

- I am very comfortable with my de-identified health data being used for health research purposes. (26%)
- I feel moderately comfortable with my de-identified health data being used for health research purposes. (38%)
- I feel somewhat uncomfortable with my de-identified data being used for health research purposes. (23%)
- I am extremely uncomfortable with my health data being used for health research purposes, even if it’s de-identified. (13%)
Patients care a lot about medical record access.
A majority of patients say that it is very important for them to have access to their own medical records.

**What is Individual Access Services?**

Individual Access Services (IAS) refers to the mechanisms and processes that enable individuals to access and manage their own health information. Health data exchange involves the sharing of electronic health records (EHRs) and other health-related information among healthcare providers, organizations, and IT systems.

IAS aims to empower patients and give them control over their health information. These services promote patient engagement and enable patients to actively participate in their own healthcare management. Examples include web-based patient portals and personal health records (PHRs), which patients can access upon successful identity verification.
When was the last time you accessed any of your own medical records through a health app or patient portal offered by your provider?

- 48% Within the past 3 months
- 21% 3-6 months ago
- 14% 6-12 months ago
- 83% within the last 12 months
- 17% other
- 5% 12-24 months ago
- 4% Over 24 months ago
- 8% Never accessed

83% of surveyed patients have accessed their own records within the last 12 months.

Nearly half (48%) have accessed their own medical records in the last 3 months.

The results clearly show that patients want access to their medical records. The policy support for individual access services — which sometimes is criticized as unjustified by the level of actual patient engagement — is clearly vindicated by this level of patient interest.

Dave Cassel
Chief Customer Officer
Health Gorilla

The State of Patient Privacy: Patient Access
Patients access their own records to keep track of their own information, check for test results and immunizations, and more.

What are your goals when accessing your medical records?

- **73%** Keeping track of my own health information
- **50%** Checking for something specific like test results or immunizations
- **43%** Checking for accuracy
- **30%** Sharing my health information with medical staff or members of my care team
- **23%** Sharing my health information with family
- **15%** Sharing my health information with third parties, such as insurers, researchers, or health-related applications / services
- **6%** None, I have never accessed my medical records
Overall, patients find it easy to access their own medical records.
When accessing your medical records, which of the following best characterizes how you feel?

- **61%** Informed
  The information is intuitive and organized

- **20%** Excited
  The ability to access my own records is something I have highly anticipated

- **25%** Anxious or fearful
  The information causes additional stress about my health

- **24%** Overwhelmed
  The information is documented using medical jargon

- **7%** N/A
  I have never accessed my medical records

By and large, patients walk away from viewing their records feeling more informed.
In this broadly representative sample of the U.S. population, most people feel that it is easy to access their medical records, that they find the information they receive to be understandable, and they believe that accessing this data is important to them for many reasons.

At the same time, there is a significant degree of concern regarding the sharing of medical information without explicit consent, even with providers and payers involved in their care. While most feel that their health data is safe and secure, there are significant concerns regarding the possibility of future data breaches, with general agreement that government certification of health data exchange raises the level of confidence in data exchange.

Steven Lane, MD, MPH
Chief Medical Officer
Health Gorilla
Conclusion

As the industry prepares for broader health data exchange enabled by new permitted exchange purposes, patients must be a part of the national dialogue. Many are vocal about their concerns — the apprehension around use-cases such as payment, operations, and public health persists. With the growing number of medical record data breaches, patients are nervous about the security programs of tech companies that store their data. However, access to one's own medical record is also a critical unlock — 83% of surveyed patients have accessed their own record in the last year, a majority of whom feel more informed after viewing their own health information.

Where does this leave us? As Dr. Steven Lane suggests, "The results of this survey will be helpful for policymakers as they continue to evolve rules and regulations to support the secure exchange of health information in order to improve the experience and value of healthcare nationwide." Patients' concerns about data privacy, security, and integrity demand our attention and investment. Their desire to understand how their data will be used and shared — particularly in contexts beyond treatment — warrant a thoughtful response, such as programs educating patients about authorized exchange purposes and encouraging an open dialogue about privacy between patients and their providers. In order to build a truly patient-centered health data ecosystem, we need to empathize with patients and their concerns, build systems that protect privacy, and integrate patients into national policymaking.
Confidentiality is at the core of effective healthcare. Without the assurance of privacy, patients cannot feel safe in sharing their most personal and sensitive information.

— Dr. Vivek Murthy, U.S. Surgeon General, Department of Health and Human Services