

Achieving the Holy Grail in Health Data Management:

Harnessing Local-First and Medical Record-Centric Principles for a Superior Health Records System

(1) Secure, (2) Private, (3) Auditable, (4) Shareable, (5) Granular Access,
(6) Data Control & Ownership, (7) Compliant, (8) User-Friendly

By Dale David | Edited by AI | 051324 | Version 2.0



Abstract

In the complex landscape of healthcare, managing medical records effectively remains a significant challenge. Every day, millions of patients visit healthcare providers, generating vast amounts of medical data. This data is captured in Electronic Medical Records (EMRs)¹, which serve as modern custodians of our medical histories. However, despite their critical role, EMRs often fall short in facilitating seamless data management and interoperability.

Currently, EMRs are like isolated islands of information. They are excellent at capturing data but struggle with sharing it across different healthcare systems. Data security is another pressing concern, with EMRs often being vulnerable targets for cyber threats, resembling treasure troves all too accessible to hackers.

The problem extends beyond just data sharing and security. EMRs have been in use for decades, yet they still face issues with data ownership, user-friendliness, and comprehensive compliance with ever-evolving healthcare

regulations. Each of these challenges is like a piece of a puzzle that EMRs have yet to fit together perfectly.

This concept paper proposes a unified solution designed to address these multifaceted challenges. By integrating enhanced security protocols, improved data sharing capabilities, and robust user management features, this solution aims to revolutionize how EMRs function. It presents a holistic approach that not only secures data but also makes it easily accessible and manageable across different healthcare environments.

Imagine a system that offers a cohesive blend of security, privacy, data ownership, auditability, compliance, and user experience, enhanced further by AI compatibility. This solution is poised to tackle the existing deficiencies of EMRs head-on, providing a comprehensive framework that enhances the functionality and efficiency of medical record management.

This is not just an incremental improvement but a fundamental transformation of the medical records landscape. The goal is to move beyond the shortcomings of current systems, introducing a truly private and secure solution providing users data control and ownership.

¹ Also known as EHR (Electronic Health Records)

Problem

In our modern digital landscape, personal memories are preserved and shared with unprecedented ease, creating a stark contrast to the fragmented and inefficient way healthcare records are managed. Despite significant technological advancements, Electronic Medical Records (EMRs) often add complexity rather than simplicity to healthcare delivery. Instead of aiding medical professionals, these systems frequently become obstacles, complicating procedures and care.

Data Fragmentation and Limited Access: Within EMR systems, patient data often exists in isolated silos, separated across various healthcare providers. This segmentation prevents the formation of a complete and coherent patient history, leading to inconsistencies in care and gaps in treatment. Accessing comprehensive patient information is crucial for effective medical decision-making but remains a significant challenge in current EMR frameworks.

Dependency on Connectivity: Most healthcare systems are critically dependent on continuous internet connectivity and central servers. This reliance introduces significant vulnerabilities, as any disruption in connectivity or server failure can lead to an inability to access crucial health records. Such interruptions can compromise patient care at critical moments, underscoring the fragility of the current digital healthcare infrastructure.

Privacy and Security Concerns: The centralized storage of sensitive health data inherently increases the risk of security breaches. When these systems are compromised, they can expose personal health information, resulting in severe privacy violations and potential financial and reputational harm to both patients and healthcare institutions.

Compliance and Transparency: Navigating the maze of regulatory compliance is further complicated by opaque data management practices. The lack of transparency in how patient data is handled erodes trust and complicates the efforts to ensure that health data is managed ethically and legally. Patients and providers alike struggle with these complexities, often feeling out of control and inadequately protected under the current systems.

Poor User Experience: The user experience with many EMR systems is often anything but intuitive. Clunky interfaces and convoluted processes not only frustrate

healthcare providers but also hinder their ability to perform their duties efficiently. This poor usability can lead to increased administrative burdens and detract from the quality of patient care.

These profound challenges highlight a critical need for reevaluating how healthcare data is managed. Current systems, while technologically advanced, fail to fully support the needs of providers and patients, calling for a thoughtful reconsideration of the tools and practices in place in healthcare data management.

The Evolution of EMRs

Before delving deeper into the challenges associated with Electronic Medical Records (EMRs), let's first understand their origins.

EMRs made their debut in the 1960s, but it wasn't until the 1990s and 2000s² that they began to see widespread adoption, particularly in developed countries. Despite their long history, many EMR systems today are still based on platforms developed decades ago. While there have been improvements, these changes have often been incremental at best. For example, the user experience within many EMR systems remains entrenched in outdated methodologies that do not align with modern digital usability standards.

It's crucial to recognize that healthcare providers are not responsible for these systemic limitations. They operate within the constraints of the available EMR systems, which were initially designed in a different technological era and have not evolved sufficiently to meet current needs.

Furthermore, the reluctance to update or overhaul these systems does not solely stem from EMR providers' neglect. Security concerns are significant; transitioning from traditional, siloed setups to more integrated frameworks could potentially expose new vulnerabilities. However, this conservative approach to innovation is not merely about caution. Financial incentives also play a significant role. Siloed systems create dependencies—they lock in users, making it difficult for healthcare providers to switch systems. This lack of flexibility benefits EMR providers

² Extract - [Brief History of EMR](#)

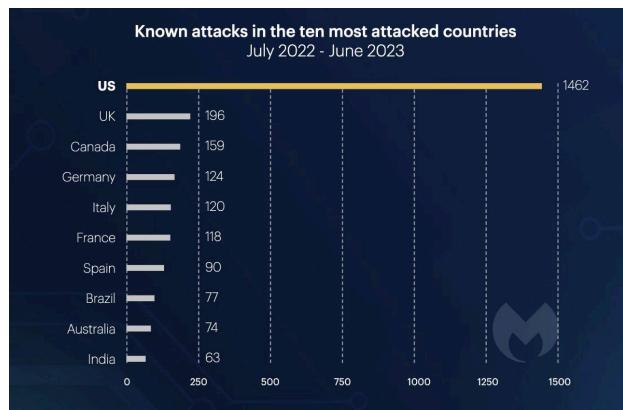
financially, as it reduces competition and discourages broader innovation in the sector.

Therefore, while technological constraints and security issues are genuine, they also mask deeper economic motivations that deter significant changes in EMR systems. This interplay between technological stagnation and economic incentives highlights the complex challenges of reforming healthcare data management.

Security Challenges

EMRs are entrusted with guarding our most sensitive medical information, acting as modern-day gatekeepers to a treasure trove of data. Yet, despite their critical role, EMRs have become a prime target for cyberattacks. In 2022, healthcare accounted for 20% of all data breaches, making it a magnet for hackers seeking to exploit vulnerabilities in data security.

The financial impact of these security breaches is staggering. By the end of 2020, they had cost healthcare organizations an estimated \$6 trillion globally. Each compromised record cost an average of \$408, underlining the high stakes involved. In the U.S. alone, over 26.4 million records were compromised in 2020³, testing the resilience of healthcare's data defenses to their limits.



Source: AppleInsider⁴

Over the past three years, a remarkable 93% of healthcare organizations have been impacted by data breaches⁵. This widespread vulnerability highlights a persistent quest among cybercriminals to capture valuable healthcare data.

The challenges are multifaceted: data breaches, unauthorized access, insider threats, interoperability issues, complex authentication requirements, and identity theft are all part of the security gauntlet that healthcare must navigate.

Adding to the drama, some hospitals have reverted to paper records following ransomware attacks, as seen in a notable incident in August 2023⁶. This step back in time not only highlights the severity of the threat but also underscores the desperate measures required to protect patient information in the wake of digital vulnerabilities.

Recent research indicates a troubling trend: a 6% increase in ransomware attacks on healthcare systems in 2023⁷. This surge underscores a growing challenge in cybersecurity, adding a complex layer to the already fraught landscape of healthcare data protection.

Data Privacy

In the digital world, personal information streams continuously, elevating the critical issue of data privacy. This isn't a trivial matter—it's about safeguarding the sanctity of personal information. At the heart of this issue is patient confidentiality, which contends with serious threats such as data breaches, medical identity theft, and internal breaches. Each incident not only compromises security but also challenges the integrity of patient trust.

Consider the implications of third-party data sharing: personal medical stories inadvertently becoming shared narratives, impacting individual privacy profoundly. The modern era of data collection and surveillance sees digital footprints evolving into complex, often indecipherable trails.

Consider the implications of third-party data sharing⁸: personal medical stories inadvertently becoming shared narratives, impacting individual privacy profoundly. The modern era of data collection and surveillance sees digital footprints evolving into complex, often indecipherable trails.

Informed consent extends beyond a mere procedural formality; it involves empowering individuals to have a say in how their data is handled and shared. Similarly, the lack of control over personal data is akin to entrusting one's

³ Tech Report - [55+ Healthcare Data Breaches](#)

⁴ Apple Insider - [Ransomware Attackers](#)

⁵ Tech Report - [55+ Healthcare Data Breaches](#)

⁶ Forbes - [Hospital System Goes Back to Paper](#)

⁷ Barracuda - [2023 Ransomware Insights](#)

⁸ HealthCareITNews - [Health Privacy Challenges](#)

secrets to a lock without a key, where personal details could be accessible by others without consent.



Cross-border data flows are complex, akin to navigating international waters, making it crucial to ensure that personal data is protected across jurisdictions. Data aggregation and anonymization pose significant privacy puzzles, requiring sophisticated strategies to maintain anonymity while utilizing data for broader benefits.

Navigating the maze of privacy regulations is comparable to executing a precise dance routine where every misstep can have legal consequences. Meanwhile, data monetization⁹ reveals that our digital footprints have significant value beyond mere social interactions, shaping a new frontier in privacy concerns.

Data Ownership

Navigating the ownership of health data¹⁰ resembles a complex dance, intertwining legal, ethical, and practical factors. The concept of ownership varies widely among different stakeholders, creating a layered and multifaceted landscape.

Patient Ownership: From an ethical perspective, patients are often seen as the rightful owners of their health data. This viewpoint supports patient autonomy and their right to control their personal information. It empowers patients to access, share, and influence the use

⁹ GlobeNewsWire - [Health Data Monetization](#)

¹⁰ Forbes - [Health Data Ownership](#)

of their health data, reinforcing the principles of patient-centered care.

Doctor/Hospital Ownership: Healthcare providers, who create and maintain health records, do not necessarily own this data. Instead, they act as stewards, ensuring the accuracy and security of the information without claiming absolute ownership.

Shared Ownership: In some instances, ownership is a collaborative effort between patients and healthcare providers. Patients maintain influence over their health data, while providers manage and use the information to enhance patient care.

Legal Ownership: Legal frameworks define who owns health data, and these regulations vary by country. Some jurisdictions recognize individual ownership, while others view the data as jointly held by both providers and patients.

Consent and Control: Regardless of the legal definitions of ownership, patient consent and control are paramount. Consent acts as a gatekeeper, granting providers temporary access to data while ensuring ultimate control remains with patients.

Healthcare Records vs. Raw Data: There is a critical distinction between healthcare records, which consist of compiled medical information, and raw data, such as individual test results. While healthcare facilities may own the records, legislation often protects patients' rights to access and manage them.

Impact of Cloud-Based Third Parties: The involvement of cloud-based third-party providers introduces additional complexities regarding ownership and access. Although contractual agreements govern these relationships, issues like cloud downtime can interrupt the flow of data and affect its usability.

Auditability

Navigating the auditability of health data can feel like unraveling a complex mystery. Effective mechanisms to audit and control the use of health data are rare, making transparency in healthcare data management akin to searching for a unicorn.

Imagine this: EMR providers frequently do not provide access logs or audit trails, obscuring the behind-the-scenes

activity regarding who accesses your data and when. This opacity significantly hampers patient empowerment, akin to attending a magic show without ever knowing what occurs backstage. Patients face significant barriers in controlling access to their data—it's like encountering a locked door with no key available to open it or control who else might enter.



Moreover, where security logs are provided, they often feel incomplete, like a detective novel missing crucial chapters. These logs, even when available, fail to guarantee that the data has been handled appropriately. The situation is further complicated in cloud setups, where visibility into data handling feels as exposed as a window without blinds, leaving personal data potentially vulnerable to prying eyes.

In essence, the trail of health data remains shrouded in secrecy, locked away without sufficient transparency or tools for patients to understand or control how their information is used.

Data Control + Granular Access

Having ownership of health data doesn't necessarily equate to having control over it, especially when it is stored within a health system managed by an external IT provider. Here's the plot twist: unauthorized access and snooping can occur within health facilities, often perpetrated by users who have general access to medical

records¹¹. This risk extends beyond facility administrators to include the main IT providers themselves.

Once a medical record is shared within a facility, it effectively becomes fair game for anyone with access. The current systems typically lack stringent limits or boundaries—patient records are left wide open, often without the patients themselves being aware of this exposure.

Empowerment is crucial in this context. Patients, alongside their attending physicians, should be at the helm, controlling who gets a "backstage pass" to their data and specifying the purposes for which it is accessed. This approach would ensure that access to sensitive medical information is not just a privilege of employment or position but is carefully weighed and granted based on clear, justified needs.

Granting granular access¹² isn't just about restricting who can see the data; it's about setting layers of permissions that reflect the sensitivity of the information and the roles of individuals seeking access. For instance, while a nurse might need access to a patient's medical history for treatment purposes, the level of detail they can see could be less than that available to the primary physician.

In essence, transforming data control from a broad and often unchecked access model to one characterized by precision and personalization is pivotal. This shift is not just about protecting privacy; it's about reinforcing trust and accountability in healthcare, ensuring that every access point to patient data is necessary, justified, and, most importantly, consensual.

Data Fragmentation

Imagine your medical information scattered like puzzle pieces across different platforms. Welcome to the realm of data fragmentation¹³, where health records often resemble a jigsaw puzzle missing crucial pieces. Instead of presenting a unified picture, what emerges are isolated islands of data, lacking the connections necessary for comprehensive healthcare.

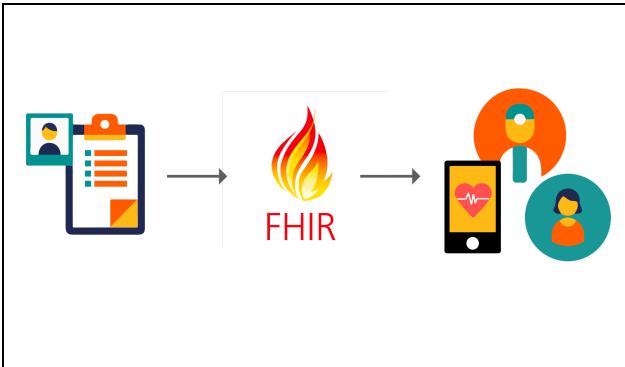
This scenario unfolds both within single healthcare institutions and across various organizations. The result is

¹¹ TheGuardian - [Stalker Doctor](#)

¹² National Library of Medicine - [Granular Access](#)

¹³ Insider - [Health Data Fragmentation](#)

a complex challenge for healthcare professionals: they must piece together a patient's history, diagnoses, and treatments from these disparate fragments. Imagine a doctor attempting to provide optimal care with only partial



insights—leading to duplicated tests and suboptimal health outcomes. It's akin to attempting to perform a symphony without all the musicians in tune.

The Rise of Interoperability Solutions

Enter the hero of this story: Fast Healthcare Interoperability Resources (FHIR)¹⁴, an initiative supported by the Office of the National Coordinator for Health Information Technology (ONC). FHIR isn't just another acronym—it represents a transformative shift in healthcare communications. It aims to establish a common language that all healthcare systems can use, enabling data to flow seamlessly between platforms. As described by the ONC, FHIR simplifies the creation of applications and supports real-time interoperability, thereby easing the learning curve for developers.

Interoperability strives to integrate these data islands into a harmonious symphony of patient care. Initiatives like FHIR take the spotlight, providing familiar frameworks that promote smoother interactions within the healthcare ecosystem. However, the journey is not without its hurdles—technical and budgetary constraints, especially among smaller healthcare providers, continue to impede widespread adoption.

Moreover, efforts like Carequality.org have emerged, seeking to connect healthcare networks across the nation and foster more integrated data handling. But a critical piece remains elusive: patient empowerment. Current systems often prioritize provider convenience over patient engagement, leaving vital issues such as consent and personal data management in the shadows.

¹⁴ HealthIT.gov - [Interoperability](#)

As the healthcare industry evolves, enhancing data accessibility remains central to progress, with the ultimate goal of orchestrating not just better healthcare, but better lives for patients.

Compliance

EMR providers navigate a complex regulatory rhythm, mastering a comprehensive range of healthcare compliance requirements¹⁵ that ensure patient data security, privacy, and effective management. The stage for this intricate dance is set by pivotal regulations that serve as the guardians of sensitive health information.

Leading the cast are the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). These acts set stringent rules, acting like vigilant sentinels that protect health data against misuse and breaches.

But the regulatory spotlight doesn't stop there. Data protection also takes center stage with regulations tailored for specific regions. For instance, the General Data Protection Regulation (GDPR) governs data protection in Europe, while the California Consumer Privacy Act (CCPA) plays a similar role in the United States.



¹⁵ Harvard Medical School - [Compliance & Data Security](#)

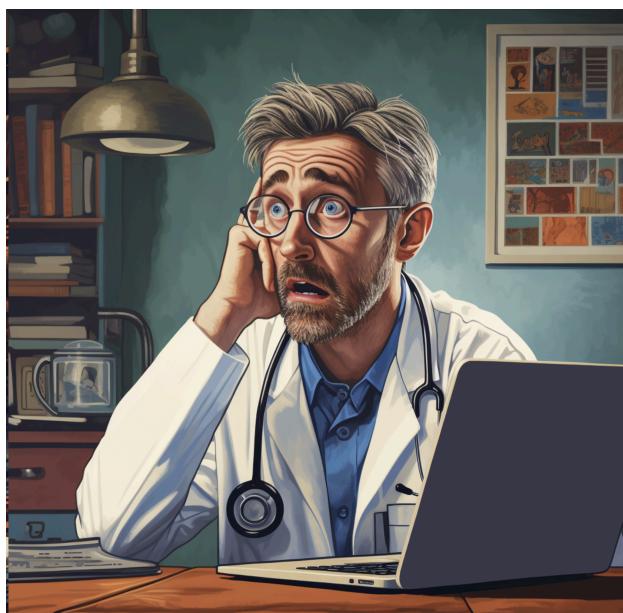
Additional performers in this regulatory ensemble include medical device regulations and standards for clinical data exchange, such as Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR), which facilitate data interoperability. Programs like Meaningful Use (now known as Promoting Interoperability) also contribute, enhancing patient care by incentivizing the effective use of EMRs.

To stay in step with these regulations, EMR providers implement several key measures: data encryption, stringent access controls, comprehensive patient consent management, and robust audit trails. Together, these measures form a choreographed routine of risk assessments and compliance checks that ensure the dance of data management does not miss a beat.

The performance is continuous, with ongoing monitoring, meticulous vendor management, and rigorous staff training keeping the momentum alive. In the realm of healthcare data management, EMR providers do more than just comply with regulations; they perform a sophisticated waltz, gracefully balancing patient data security and privacy throughout their operations.

User Experience

Navigating the world of Electronic Medical Records (EMR) systems can often feel like entering an intricate maze



fraught with challenges¹⁶. Here's a deeper look into the

healthcare practitioner's journey through this complex landscape:

Complexity Conundrum: EMR interfaces can be as confusing as a bustling city with too many streets, causing users to lose their way. Fields, tabs, and options accumulate, transforming the path to critical patient data into a labyrinthine ordeal. This complexity can lead to frustration and wasted time, obstructing swift access and diminishing the system's overall efficacy.

Data Entry Dilemma: Data entry should be straightforward, but often it's like wrestling with a stubborn lock. Healthcare professionals spend precious time inputting data, and cumbersome systems further sap efficiency. Worse yet, usability flaws exacerbate these challenges, leading to interfaces that not only slow down tasks but also increase the likelihood of errors.

Customization and Connection: Lack of customization forces practitioners into ill-fitting workflows, akin to wearing shoes two sizes too small. Moreover, when systems fail to communicate effectively with each other, patient data becomes disjointed—resulting in missed appointments and incomplete records.

Speed Bumps & Learning Leaps: Encountering slow interfaces adds unnecessary delays. In the fast-paced world of healthcare, any sluggishness disrupts the workflow rhythm. For newcomers, mastering EMRs is like scaling Mount Learning Curve, as they navigate complexity while striving for efficiency.

Alert Overload & Documentation Drama: Constant alerts can overwhelm, like being in a room where every alarm clock goes off at once. Excessive documentation requirements are equally burdensome, forcing healthcare professionals to push a metaphorical boulder uphill, diverting their focus from patient care to paperwork.

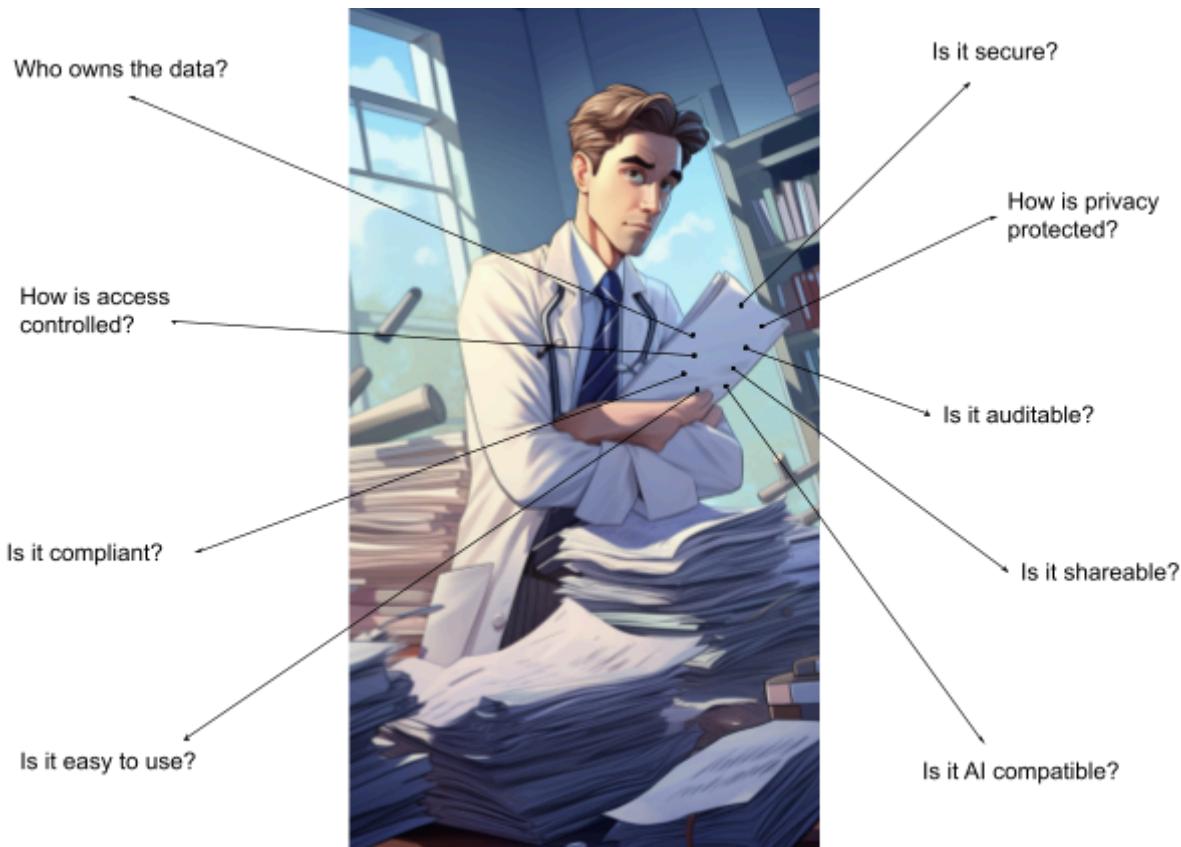
Design Dilemmas: The solution lies in embracing user-centric design. Involving healthcare professionals in the design process, conducting regular user testing, and sprinkling in some customization can transform EMR interfaces into tools that fit like a glove.

In conclusion, crafting a smooth EMR experience is not merely about deploying advanced technology—it's about creating systems that streamline healthcare processes, reduce stress, and elevate patient outcomes.

¹⁶ Journal of User Experience - [Usability of EMR](#)

There are Billions of Medical Records across the globe. And millions more are being created every day.

The following diagram shows the huge gaps that need to be addressed:



**Many Healthcare Providers around the world are still using paper-based or analog systems.*

It's about time that a system-agnostic platform is built to address all these gaps once and for all.



Excerpt from Reed Jobs Interview with Dean Lloyd Minor (March 2022)

Reed Jobs, the former Managing Director of Health at Emerson Collective, eloquently highlighted the concerns regarding medical records during his interview¹⁷ with Dean Lloyd Minor of Stanford Medical School.

*"I think one of the most important things we can learn is that we need to really **respect people's privacy** and we need to give them the **power to determine who has access to their data** and what that's used for.. and so it's interesting when you look at healthcare, clinical records, and **most data that flows** through hospital systems, it is **absurdly balkanized and the user interface is atrocious**, and it's kind of this surreal experience honestly because we live in a wonderfully high-tech world and particularly here in Silicon Valley, yet when you go to a hospital, even a great hospital like Stanford, it's like you're **stepping back in a time machine 30 years** and you know the software there is nothing against everybody, the software's not very, not very good, the user interface isn't very good, and it's this, you know, **departments can't talk** to each other, and **you can't transfer data**, and people give you*

floppy disks with things on it, and it's like this anachronistic little, you know, little time machine, it's crazy.

*So I think one of the most interesting things that's going to happen in healthcare in the next kind of 20 years is seeing it really catch up with the rest of the world from a technological point of view just **both from a data infrastructure interoperability and UI aspect**, and I really hope, and luckily, this is a lot of this is already codified in legislature like HIPAA and stuff, but **people's privacy and control over that data is gonna need to be paramount** as it, you know, it currently is now, but it **really needs to be a lot more electronic and it needs to be a lot more interoperable**, again, this is something that's probably, you know, a nationwide, you know, level, whether that's through legislation or **through some really innovative companies in the space** of which I think there's space for many, but yeah, we need to, we need to really shape up the, the, the infrastructure systems that we have in place because, not only are they really not helping patient care, but it's, it's really bad for the hospital systems themselves too and the physicians.." - Reed Jobs*

¹⁷ Stanford Medicine - [Emerson Collective Reed](#)

Solution

Can we effectively resolve the complex challenges inherent in Electronic Medical Records (EMRs)? The "Holy Grail" of EMR solutions proposes a comprehensive approach—not merely patching existing problems but addressing the underlying issues head-on, enabled by advances in technology that were not previously available.

This solution envisions a scenario where data security and the ability to share information are not competing goals but are integrated features. The "Holy Grail" advocates for a system where data can flow freely yet remains protected under stringent privacy measures. Advances in Local-first technologies now allow for sophisticated local data processing and storage solutions that maintain high levels of security and accessibility, overcoming limitations that previous technologies could not.

At the core of this transformative solution are two pivotal concepts: the "Local-First" approach and the "Medical Record-Centric" philosophy. The Local-First approach promotes a collaborative environment built on data ownership, enabling healthcare professionals and patients to work together seamlessly. This approach minimizes the risks associated with centralized data storage and reduces dependencies on constant internet connectivity. By leveraging local processing and decentralized data management, it mitigates vulnerabilities that can lead to data breaches and access disruptions—challenges that were insurmountable with earlier technological frameworks.

Meanwhile, the Medical Record-Centric philosophy focuses on placing the medical record at the center of the EMR system. This approach enhances the usability and functionality of EMRs by streamlining interfaces and improving the logical flow of data access. It ensures that patients' medical histories are complete and easily accessible, crucial for delivering consistent and effective medical care.

Together, these innovative principles not only address the fundamental issues of security and privacy; they also tackle problems of data fragmentation and enhance user interfaces. By optimizing data control, these strategies empower both patients and healthcare providers, making the management of healthcare data more transparent and compliant with regulatory standards.

The EMR "Holy Grail" is more than an abstract concept; it is a practical and actionable pathway that transforms existing challenges into opportunities for systemic improvement. By embracing this approach, powered by the latest advancements in Local-first technology, we are not only envisioning potential futures but are actively creating a new reality for healthcare. This journey towards a reimagined EMR system is reshaping the landscape, making healthcare more integrated, secure, and patient-focused.



Local-First Approach

The Local-First approach represents a paradigm shift in software design, emphasizing both collaboration and ownership directly on the user's device. This approach integrates critical principles from the Local-First software philosophy, focusing on enhanced data control, security, and operational resilience regardless of network availability¹⁸.

In this model, software systems prioritize device-based processing and storage, reducing dependency on cloud servers. This shift ensures that applications continue to function effectively, even in offline scenarios, thereby



VIDEO: ARDHIRA PUTRA

GREGORY BARBER BACKCHANNEL AUG 3, 2023 6:00 AM

The Cloud Is a Prison. Can the Local-First Software Movement Set Us Free?

maintaining user productivity without interruption due to connectivity issues.

The device-centric model not only enhances data accessibility but also significantly increases data privacy and security. By keeping data localized, the exposure to breaches associated with centralized data storage is minimized. Moreover, this model supports real-time data manipulation, allowing users to update and access their information instantaneously.

One of the principal technological underpinnings of the Local-First approach is the implementation of

Conflict-free Replicated Data Types (CRDTs). CRDTs are advanced algorithms designed to keep data consistent across multiple devices without needing centralized coordination. They seamlessly handle concurrent data updates, which are typical in collaborative environments, and resolve potential conflicts without user intervention, ensuring data integrity is maintained across all nodes.

The benefits of the Local-First approach extend beyond just improved data access and security. It enhances overall system responsiveness and user experience by eliminating delays inherent in server-based data fetching. Additionally, it aligns with regulatory requirements by simplifying data sovereignty concerns—data resides on the user's device, aligning with jurisdictional privacy standards.

The adoption of the Local-First approach addresses significant challenges in data management, including ownership disputes and privacy concerns, by empowering users with control over their data and reducing reliance on third-party data processors.

Local-First Software: You Own Your Data, in spite of the Cloud

Martin Kleppmann
Department of Computer Science and Technology
University of Cambridge
Cambridge, United Kingdom
martin.kleppmann@cam.ac.uk

Peter van Hardenberg
Ink & Switch
San Francisco, CA, USA
pvh@inkandswitch.com

Adam Wiggins
Ink & Switch
Berlin, Germany
adam@inkandswitch.com

Mark McGranaghan
Ink & Switch
Seattle, WA, USA
mark@inkandswitch.com

Abstract
Cloud apps like Google Docs and Trello are popular because they enable real-time collaboration with colleagues, and they make it easy for us to access our work from all of our devices. However, as our data storage on servers, cloud apps also take away ownership and agency from users. If a service shuts down, the software stops functioning, and data created with that software is lost.
In this article we propose *local-first software*, a set of principles for software that enables both collaboration and ownership for users. Local-first ideals include the ability to work offline and collaborate across multiple devices, while also improving the security, privacy, long-term preservation, and user control of data.
We survey existing approaches to data storage and sharing, ranging from email attachments to web apps to Firebase-backed mobile apps, and we examine the trade-offs of each. We look at Conflict-free Replicated Data Types (CRDTs): data structures that are multi-user from ground up while also being fundamentally local and private. CRDTs have the potential to be a foundational technology for realizing local-first software.
We share some of our findings from developing local-first software prototypes at the Ink & Switch research lab over the course of several years. These experiments test the viability of CRDTs in practice, and explore the user interface.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for works published in this journal are held by the author(s) or other copyright holders. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission from permissions@acm.org.
© 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6495-4/19/10...\$15.00
<https://doi.org/10.1145/3359591.3359737>

challenges for this new data model. Lastly, we suggest some next steps for moving towards local-first software: for researchers, for app developers, and a startup opportunity for entrepreneurs.

CCS Concepts → Human-centered computing → Collaborative content creation; Ubiquitous and mobile computing systems and tools; Computer systems organization → Peer-to-peer architectures; Software and its engineering → Peer-to-peer architectures; Organizing principles for web applications

Keywords: collaboration software, mobile computing, data ownership, CRDTs, peer-to-peer communication

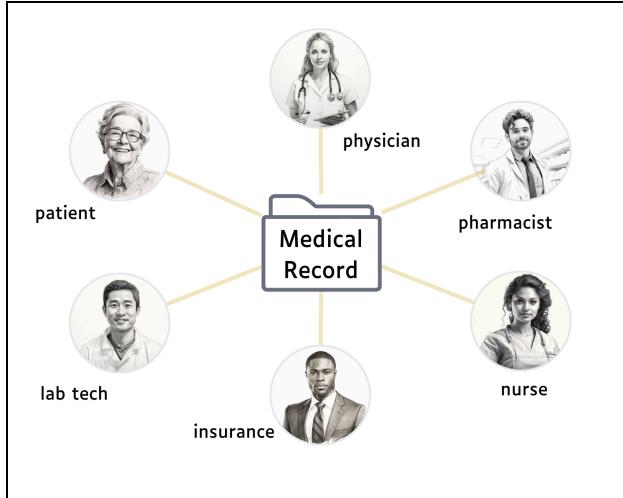
ACM Reference Format:
Martin Kleppmann, Adam Wiggins, Peter van Hardenberg, and Mark McGranaghan. 2019. Local-First Software: You Own Your Data, in spite of the Cloud. In *Proceedings of the 2019 ACM SIGPLAN International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software (Onward'19), October 23–24, 2019, Athens, Greece*. ACM, New York, NY, USA, 25 pages. <https://doi.org/10.1145/3359591.3359737>

1 Motivation: Collaboration and Ownership
It's amazing how easily we can collaborate online nowadays. We use Google Docs to collaborate on documents, spreadsheet, and presentations. Figure 1 shows together on our interface designs, we communicate with colleagues using Slack; we track tasks in Trello; and so on. We depend on these and many other online services, e.g. for taking notes, planning projects or events, remembering contacts, and a whole raft of business uses.
We will call these services "cloud apps," but you could just as well mean "Software as a Service" (SaaS) or "web-based." What they have in common is that we typically access them through a web browser or through mobile apps, and that they store their data on a server.

*Local-First Software White Paper

¹⁸ Ink & Switch - [Local-First Software](#)

Medical Record Centric



In the domain of Electronic Medical Records (EMRs), the focus has traditionally been oriented towards healthcare providers, with a gradual shift to include patients more actively. Despite these changes, challenges related to medical record ownership and seamless sharing remain prevalent.

Developed by Team EasyJoey, the 'Medical Record-Centric' approach proposes a strategic shift to simplify these complexities. It centers on the medical record itself—making it complete, interconnected, and the core focus of the EMR ecosystem.

Collaborative Synergy: Inspired by the real-time collaboration seen in tools like Google Docs and Trello, this approach introduces similar capabilities to EMRs. It empowers physicians and patients to collaborate effectively, leveraging the strengths of FHIR for coherent data integration and a Local-First methodology for data management. This setup enables physicians to initiate collaborative sessions effortlessly, enhancing the fluidity of information sharing and improving the efficiency of healthcare interactions.

Precision Access Management: In this model, control over data is paramount. The 'Medical Record-Centric' approach adopts granular access control, allowing users to precisely manage who can access, edit, or interact with specific parts of their medical records. This level of control enhances privacy, supports active collaboration, reduces security risks, ensures compliance, and tailors data-sharing to individual preferences. The system

employs a sophisticated array of credentials, roles, and privileges, empowering users to direct their medical data's journey meticulously.

Guardians of Encryption: Security is a cornerstone, with end-to-end encryption protecting each medical record during collaborative activities. This security measure ensures that only authorized individuals can access the shared information, akin to the encryption protocols used in apps like Telegram. This layer of cryptographic security provides a robust defense against unauthorized access to sensitive medical data.

Path of User Documentation: Transparency is critical in this approach. The User Trail Documentation feature meticulously logs every interaction with patient data, providing detailed insights into access, modifications, and viewing activities. This feature helps detect and address suspicious activities swiftly, enhancing accountability and protecting data integrity. Further bolstering auditability, blockchain technology is utilized to store transaction proofs, offering a formidable barrier against data tampering.

User Experience Refinement: User experience is crucial in healthcare. The 'Medical Record-Centric' approach redefines patient data management with an intuitive, well-designed interface that minimizes errors and optimizes workflows. Echoing the simplicity and efficiency of Google Docs, this interface facilitates a smoother user interaction, ultimately enhancing patient care and satisfaction.

Optional Timestamping in Blockchain

In this context, blockchain technology serves a supplementary role, enhancing auditability rather than acting as the foundational technology of the solution.

The concept centers on embedding timestamped records of critical health transactions on a secure private blockchain. These transactions specifically refer to the exchange of medical records from one doctor or facility to another, ensuring that each transfer is documented and verifiable. This innovative strategy aims to construct a comprehensive network of timestamped transaction proofs within the blockchain, significantly increasing both transparency and accountability.

By leveraging the inherent characteristics of blockchain technology, the timestamps and their associated

transaction proofs become immutable and resistant to tampering. It is crucial to note that this blockchain is not designed to store actual health records. Instead, its primary function is to maintain a pristine ledger of transaction proofs, confirming the integrity of each record exchange without compromising the privacy of the underlying data.

The proposed operational model envisions the establishment of a private blockchain structured as a Decentralized Autonomous Organization (DAO). Esteemed healthcare entities are invited to join this consortium, enhancing transparency and governance standards collectively. A separate paper will explore the operational details and implications of this DAO-based private blockchain, providing clarity on its structure and functionality.

This approach significantly bolsters the system's auditability, ensuring a detailed and indelible trail of all record exchanges between healthcare providers. The use of blockchain for timestamping these transactions introduces an additional layer of credibility and security, reinforcing the overall trustworthiness of the EMR system.

Compliance

In the landscape of Electronic Medical Records (EMRs), compliance is not merely a requirement but a foundational pillar essential for building trust and ensuring security. The proposed EMR system rigorously aligns with a broad spectrum of stringent compliance regulations and leverages the strengths of the Local-First and Medical Record-Centric principles to enhance its adherence.

The system meticulously meets the mandates of the Health Insurance Portability and Accountability Act (HIPAA) and the requirements outlined by the Health Information Technology for Economic and Clinical Health Act (HITECH). It also aligns with global data protection regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. Furthermore, it is compliant with the Fast Healthcare Interoperability Resources (FHIR) standards, ensuring that the solution is interoperable with other healthcare systems, thus facilitating seamless data exchange across diverse healthcare environments. Such comprehensive adherence underpins the system's robust stance on compliance.

The Local-First approach supports compliance by

maintaining data locally on the user's device, minimizing the risks associated with central data storage and unauthorized access. This principle ensures that personal health information is protected by default, with data accessibility and control remaining firmly in the hands of the user, thereby aligning with privacy regulations that prioritize data sovereignty.

The Medical Record-Centric approach facilitates compliance by focusing on the medical record as the core unit of the system. This focus ensures that all interactions with patient data are tracked and documented, enhancing audit trails and making it easier to adhere to compliance requirements. By prioritizing the integrity and accessibility of medical records, this approach supports stringent regulatory standards for data handling and patient privacy.

Achieving compliance within EMRs extends beyond simply ticking regulatory checkboxes. It involves the seamless integration of advanced data protection measures into the system's architecture. This includes robust data encryption, stringent access controls, detailed consent management, and comprehensive audit trails. These mechanisms are not just supplementary features but are woven into the very fabric of the EMR system, ensuring that compliance is intrinsic to every operation.

The commitment to compliance signifies a profound dedication to maintaining the highest standards of security, privacy, and ethical data handling. By meticulously implementing these safeguards and continuously updating them to meet evolving standards, the EMR system fosters unwavering trust among healthcare providers, patients, and stakeholders. In the realm of healthcare, where trust is paramount for therapeutic relationships, this steadfast commitment to compliance forms a critical cornerstone. The proposed EMR solution, enhanced by Local-First and Medical Record-Centric principles and compliant with FHIR, is dedicated to reinforcing this foundation, thereby enhancing the overall efficacy and reliability of healthcare delivery.

Medical Records Landscape

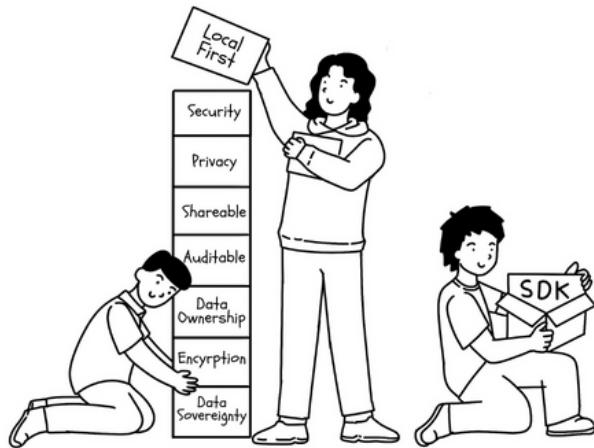
In the evolving healthcare technology sector, understanding the landscape from the perspective of healthcare providers is essential. The solution proposed in this concept paper introduces a pioneering category: the Local-First Health Records System. This innovative approach doesn't just add to the existing options but creates and leads a new path.



Challenges Faced by Providers: Healthcare providers often grapple with EMR systems that are either too cumbersome or overly complex, especially for small to mid-sized practices. These existing systems, dominated by established giants, frequently require significant investments in terms of money and time, posing substantial challenges for adoption and integration. Additionally, many systems focus on specific aspects of EMR functionality such as security or interoperability but fail to offer a holistic solution that addresses all operational needs comprehensively.

A New Category: The local-first Health Records System proposed by this concept paper is the first of its kind, designed to address the multifaceted demands of healthcare providers by integrating Local-First and Medical Record-Centric approaches. This system stands out by offering a seamless blend of user-friendliness, robust security, and enhanced collaborative capabilities, all optimized for real-time accessibility and data sovereignty.

Simplifying Adoption: Recognizing the hurdles in adopting new technologies, this innovative solution simplifies the transition for healthcare providers. It reduces the dependency on continuous training and the need for extensive technical support, facilitating quicker adaptation and integration into daily operations. This ease of adoption is particularly crucial for smaller providers, who benefit most from the system's scalability and ease of use.



Leadership and Vision: By establishing a new category of EMR systems, this solution is not merely competing with existing technologies but is setting a new standard and direction for the industry. It is designed not only to meet current regulatory and operational demands but to anticipate future challenges and innovations in healthcare technology. As the first to forge this path, the Local-First Health Records System positions itself as a leader, inviting other players in the market to follow its lead in prioritizing provider-centric, flexible, and secure health data management.

Opportunity for Transformation: As the healthcare landscape continues to shift, the demand for adaptable, efficient, and secure EMR solutions grows. The introduction of a Local-First Health Records System marks a significant opportunity for transformation in the sector, providing a model that other systems will likely strive to follow. It represents a compelling invitation for stakeholders across the healthcare spectrum to align with a solution that is not just another option but a trailblazer, poised to redefine how health records are managed and utilized.

Project 'Local-First Health'



Local-First Health (LFH) is an initiative committed to enhancing health records management and ensuring data sovereignty through technological innovation. By adopting local-first principles, LFH ensures that data remains secure and private, stored on the user's own device rather than in the cloud. This approach facilitates seamless collaboration and data shareability, empowering healthcare providers and individuals to manage and control their medical data confidently.

Firstly, LFH will apply local-first principles to address inefficiencies and security vulnerabilities in current health records management systems. This method reduces reliance on constant internet connectivity and mitigates risks associated with data breaches.

Secondly, the initiative introduces 'Project Papaya,' an innovative open-source Software Development Kit (SDK) for Medical Records Management. This SDK empowers developers to create customized medical records applications with ease, improving the accessibility and affordability of EMR solutions. Being open source, Project Papaya welcomes continuous community-driven improvements, ensuring it remains responsive to the needs of various healthcare providers.

Thirdly, LFH plans to establish a community-driven platform that will serve as a collaborative hub for innovators and developers. This platform will support the sharing of healthcare applications and code, fostering the growth and adoption of local-first healthcare solutions throughout the industry.

The team behind Local First Health brings a wealth of experience, having been active in the healthcare records space since 2016. Their prior work includes developing a 'traditional' Electronic Medical Record (EMR) system with inherent offline capabilities, alongside building a robust healthcare API infrastructure. These projects have provided critical insights and highlighted areas for potential enhancements.

With their extensive experience and the growing interest in local-first technology, LFH is poised to significantly enhance how healthcare providers access and manage medical records. The initiative aims to build a community focused on developing health tech tools that improve healthcare access globally, ensuring that individuals can securely access their medical records whenever needed.

For ongoing updates, please check:
www.localfirsthealth.org
Email: localfirsthealth@gmail.com

Local-First Health | San Francisco, CA