# Are electronic health records useful yet?

2 March 2020, by Jen Pinkowski

Credit: Javier Larrea/Alamy Stock Photo

On Friday, July 19, 1907, a grand experiment began at Mayo Clinic in Rochester, Minnesota. As the first patients of the day arrived, doctors assigned each of them a unique number and started a medical chart, noting the chief complaint, symptoms, any diagnosis, and occasionally a treatment plan.

Patient 004, a 48-year-old woman, complained of pain and tenderness in her abdomen. Having her medical dossier on hand proved useful two months later when she returned to the clinic and had her gallbladder removed.

Assigning a patient a number and a collated medical record may sound unremarkable. But in 1907, the creation of a numeric registration system tied to a single dossier—in which any clinic doctor could find a patient's entire medical history in one place—represented a huge innovation in healthcare.

Mayo, which traces its roots to 1889, began as a family practice created by Dr. William W. Mayo and his sons. It evolved into one of the world's first integrated group practices, where physicians specialized in particular areas of care and worked together to treat patients; it was this model that made necessary a single record accessible to all of the caregivers treating each patient.

The new chart system, conceived by Dr. Henry S. Plummer and his assistant, Mabel Root, became the basis for Mayo Clinic's medical record infrastructure, which now contains more than 9 million electronic health records (EHR) at the Rochester facility alone. And more records are always being generated: more than one million people visit Mayo Clinic every year.

Plummer's insight was twofold, says Cris Ross '88, the chief information officer for Mayo Clinic. "If we had a shared ledger that everyone could use, we could improve the care for patients—but also systematize the data so that we could draw insights from it," he says.

As Plummer's system did in the 20th century, EHRs are supposed to revolutionize healthcare in the 21st century by giving each one of us a single dossier containing our entire medical history—comprehensive, portable, accessible, and shareable among patients, physicians, insurance companies, pharmacies, labs, caregivers, and researchers.

But the reality is that most of our health records are scattered across disconnected systems. They're often hard to access, riddled with privacy concerns, vulnerable to security breaches, and have the potential to be sold, transferred, or monetized without our knowledge. And despite federal and state laws aimed at improving access and security, the full potential of EHR always seems to be a few years away.

The story of EHRs serves as a prelude of to what we're experiencing today in almost every facet of our lives: a utopian promise of ubiquitous data tempered with technical challenges and concerns over privacy. They have proven to be a canary in the coal mine, an early indicator of the complexities of managing the huge amounts of data we produce as we go about our lives in an increasingly digitized world.

In 1996, President Bill Clinton signed into law the Health Insurance Portability and Accountability Act,

or HIPAA. The main legal instrument for patient healthcare rights, HIPAA had two main purposes: to improve people's ability to maintain health insurance between jobs, and to make healthcare organizations responsible for the privacy of their patients' healthcare data, which was increasingly in digital form—especially in hospitals. At the time, most doctor's offices were still relying on paper records, says Ross. "The ability to share data when it was paperbound was just insurmountable," he says.

From 2001 to 2011, the number of EHRs increased 57% percent. The most significant push for EHRs emerged in early 2009 with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, the Obama administration's stimulus package. Since then, HITECH has paid out tens of billions in financial incentives for healthcare professionals to adopt EHRs. It's also bolstered penalties for HIPAA violations.

The use of EHRs in doctor's offices nearly doubled between 2009 and 2017, to almost 86%. Hospitals fared even better, with 95% adopting certified EHRs by 2017.

Imagine a comprehensive view of your health over a lifetime, with all the records united, accessible, and portable. Every vaccination you got as a baby; the broken arm you got from falling off your bike; the eye exam that revealed your nearsightedness; the blood test that found your thyroid is underperforming; the ER visit for food poisoning; the prescriptions you received for antibiotics, birth control, or high blood pressure. Today, many EHR include not only your personal information but professional guidance for physicians, including best practices, prompts, and checklists.

But creating and using effective EHRs is a technical challenge.

"Healthcare data is orders of magnitude more complex than might exist around a consumer of some other product or service," says Ross. "Understanding who you are as a customer of a bank, or an airline, or a hospitality company is relatively straightforward compared to the extreme complexity of medical data. We're facing a significant challenge in just explaining the facts about a patient from one doctor to another."

One major issue is interoperability, or the ability of different EHR systems to communicate with each other. This issue emerged soon after HITECH began offering incentives; to get these, healthcare providers needed to use a government-certified EHR system. But well over 500 systems were certified. Today, most healthcare providers use the same half-dozen EHR systems, Ross says, and interoperability has improved, but it remains limited. That's why the National Coordinator for Health Information Technology has proposed new regulations aimed at improving shareability of EHR.

There are some areas of interoperability success. For example, doctors and hospitals can check your prescription history in a national medication repository run by the organization Surescripts, which is especially helpful for the care of patients who have many medications over the years.

Recently, Ross relied on Surescripts, where he was executive vice president and general manager of clinical interoperability from 2010 to 2012, to manage his mother's prescriptions. "As my mom moved between different health systems, it was extraordinarily useful to have a single listing of all of her medications, because she couldn't remember them," he says.

Rather than holding information about specific prescriptions, Surescripts is a repository of data that points to where the prescription data is kept. "In my mom's case," Ross says, "it pointed to the health system that prescribed the drugs, and it pointed to the pharmacy that issued those drugs. From that they were able to determine what was she prescribed and if she had been refilling those medications, and therefore taking them."

As yet, there are no similar national repositories of X-rays, bloodwork, lab results, EKGs, or other common practices. But they would be useful, and some have tried to create them, including Ross. "Imagine that you're admitted to an emergency department, and you're unconscious," he says. "It

would be useful to be able to find out more about you. Maybe you're unconscious because of some heart failure. Have there been tests done before? Are there EKGs?"

Approaches similar to the one taken by Surescripts "may emerge in other kinds of spaces," Ross says. "It's one of the things that would help improve care and reduce the cost of care if we didn't have to redo tests."

Another issue is usability, or how easy the systems are to use for physicians, technicians, and hospitals. "Usability is about making the practice of medicine more effective, efficient or more satisfying to physicians who have really difficult jobs," Ross says. "They expect—and they deserve—systems that support them." In the rush to digitize records, user-friendliness wasn't always a priority for health IT developers.

In 2018, Ross and his Mayo colleagues completed two multi-year projects to "radically change technology" in the system. The first was the consolidation of medical record technology previously split amongst multiple vendors onto one integrated electronic health record system. It's now used in all Mayo Clinic locations across the U.S. The goal was to have doctors, nurses, pharmacists using common technology to provide the same standard of care.

The second was the creation of a unified data platform—which is now being redesigned to operate on Google's cloud-based technology—to manage all of the data in one place. It's a single-stop storage facility for patient care, research, and education.

Ross got to see firsthand how these EHR upgrades impacted patients when he was diagnosed with stage 3 colorectal cancer—and treated at Mayo Clinic in Rochester. (He's now cancer free.) "My treatment started just two months after we had completed our electronic medical records system," he says. "The doctors, nurses and techs were just getting used to it. It was eye-opening to me to see how our doctors were struggling with our particular record."

In the years since HIPAA became law, the ever-increasing amount of data has sparked new legislation on the protection and security of patient data. The California Consumer Privacy Act, which puts significant requirements and restrictions on businesses that collect and sell customer data, went into effect on January 1, 2020. A similarly stringent bill was introduced last year to the New York senate, but it stalled in committee. Utah passed a law last year that restricts how government agencies can access data stored with third parties such as Facebook. And in Congress, both Democrats and Republicans introduced data privacy bills in late 2019.

Most health providers, including Mayo Clinic, approach EHR privacy in the same way—by de-identifying patient info, encrypting data, abiding by HIPAA regulations, and getting consent from patients to use their data for treatment, research, and payment purposes.

Just as significantly, EHRs offer patients a view into their own care. Over the last decade, many healthcare organizations, including Mayo Clinic, have created "open notes," making doctors' notes visible to the patient. "Patients who get treated at Mayo get access to their data via either our patient portal or patient app, and they can see everything—all of their labs, all of their radiology studies, all of the communications from their physicians to them and to colleagues," says Ross. "It allows patients to be pretty empowered with their own medical care and how they can use their data."

HIPAA guarantees that consumers can get copies of their medical records, generally within 30 days, and be alerted to who has seen their data. But that doesn't mean these records are necessarily easy to get. A 2019 study by researchers from the Yale School of Medicine found widespread lack of compliance with HIPAA rules at hospitals and doctors' offices; inconsistent, unclear, or missing patient guidelines for record requests; and sometimes exorbitant costs.

Older records may not even exist. Medical record retention laws vary from state to state, based on patient age at the time of treatment and whether the records are necessary to ongoing care, among other factors, but most range between three and 10

years. Records dating to childhood are often tossed soon after the patient reaches age 18.

The consumer health tech company Ciitizen aims to fill that gap. Two years ago, the company created an online platform for cancer patients to collect, store, and share their medical data in one place. Ciitizen is free, and—crucially—it tracks down medical records on behalf of its users. Its founder, Anil Sethi, left his job as the director of Apple Health to care for his sister, Tania, who was diagnosed with, and later died of, breast cancer.

"We use the HIPAA right of access that empowers patients to get all of their medical records, and any records that are used to make decisions about patients, including images, pathology reports, genomic test results, labs, medications, notes—everything that isn't a business record," says Deven McGraw, Ciitizen's chief regulatory officer. From 2015 to 2017, she was the deputy director for health information privacy at the Office for Civil Rights in the U.S. Department of Health and Human Services (HHS), which enforces HIPAA regulations.

Ciitizen users sign a form letter drafted by the tech company so that the records request originates from the patient. Then Ciitizen uses old-school methods to gather records for its high-tech platform: phone calls, mailed letters, emails, even faxes. "I call it doing it the hard way," McGraw says. "It's very old fashioned."

Ciitizen has kept track of the HIPAA compliance rate of the medical record providers they've contacted. The result is a "scorecard" of how well about 200 facilities—including a few locations of Mayo Clinic—did in responding to their requests.

After compiling the raw data, which is stored on Amazon Cloud Services and can total many thousands of pages for a single person, "we go into the records through a combination of human and natural language processing software, pull out the relevant elements, and standardize them," McGraw says. "So people have this nice cancer summary that they can provide to another physician or to see if they're eligible for a clinical trial."

Their data is sometimes sold. "If the Ciitizen user has said, "Yes, I will share my data with this pharma company for this purpose' or has told us, "I'll share my data generally with pharma companies," then that's how we make money. The commitment that we're making to our users is that their data does not go to any third party without their consent."

Ciitizen may have its protections in place, but a lot of personal health data is going to third parties without user consent. As a 2019 paper documented, these so-called shadow health records are generated by many sources, including our own digital activity—fitness trackers, web searches, shopping histories, social media posts, health apps, and consumer genetic services like 23andMe.

Ciitizen isn't covered by HIPAA but by the Federal Trade Commission under the FTC Act, which prohibits unfair or deceptive trade practices. Many of the companies collecting these shadow health records reside in this same gray area. "I'd be happy to be covered by reasonable privacy laws," McGraw says. "We're just trying to empower the patients to have their data so that they too can share it in whatever way works for them."

Many in the healthcare industry are sincerely attempting to navigate these uncharted waters. But there are plenty of sharks circling as well. According to reports to the HHS, more than 38 million health records were breached in 2019 alone. Some were the result of hacking, others technical error. Even supposedly legal deals have many on edge: Google's recent "Project Nightingale" partnership with Ascension Health network gave it access to the health records of 50 million Americans, reportedly without their consent—and those records aren't de-identified. HIPAA regulators began looking into Project Nightingale and a Congressional committee asked for details about the agreement, even as Google insisted the deal was HIPAA compliant.

(As for the Mayo Clinic data stored in Google Cloud, Ross says, "Google doesn't have any right to get to that data for any kind of commercial purpose whatsoever.")

Despite its size, the healthcare industry lags behind other industries when it comes to cybersecurity. "There are still places where our systems are not as sophisticated as what you might see in finance, aerospace or retail, or other kinds of tech-leading industries," says Ross. "We obviously are highly concerned about attacks for financial purposes, where someone might want to steal the identity or payment information about our patients. We're also really concerned about nation-state attacks. We know from intelligence, security, and law enforcement organizations that those entities may be seeking data for industrial-espionage purposes. Or they might be seeking information about individuals that they can use for malicious purposes. The cyberdefense and cyberprotection environment is always challenging. Now that healthcare, like other industries, is digitized, we need to step up our ability to defend ourselves."

One of Dr. Plummer's many medical innovations at Mayo Clinic was to successfully argue for the installation of a pneumatic system there. It was through this series of tubes that patient medical records could be whooshed to another doctor within the facility.

We may no longer shoot capsules of our medical records through pneumatic tubes, but our EHRs are still shooting through our digital systems, for better or for worse.

"Everyone should be vigilant about how their data is being used, whether it's their browser history, financial purposes, or health data," says Ross. "I think the healthcare industry is getting a lot more sophisticated and a lot more capable in understanding how to pursue the kind of dual mission of 'more data drives more cures'—and yet that basic data needs to stay private."

**More information:** Carolyn T. Lye et al. Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records, *JAMA Network Open* (2018). DOI: 10.1001/jamanetworkopen.2018.3014

Provided by Yale University