WHITE PAPER

Patient Privacy and Data Governance in the Era of COVID-19

> Data accountability strategies for balancing privacy and public health.

NEXTGATE

COVID-19 is changing nearly everything about the way healthcare organizations operate. From telehealth visits and elective surgeries to staffing strategies and sanitation protocols, providers are being forced to reexamine the very basics of how they deliver care in order to protect staff and patients from a highly contagious disease.

Of course, radical reinvention is nothing new for healthcare. Over the past decade, change has been constant for an industry that has adopted digital tools at lightspeed while dramatically overhauling the way trillions of dollars move through the system.

Even something as seemingly fundamental as patient privacy has evolved alongside the digital transformation. As patient data moves out of filing cabinets and onto cloud servers, a new regulatory framework is emerging to keep data secure while encouraging organizations to share information appropriately with patients and peers.

Earlier in 2020, CMS and the Office of the National Coordinator took a major step toward realigning the patient data access environment by releasing a landmark set of final rules about information blocking and public data sharing accountability.[1]

While these rules were designed in a pre-pandemic world, they may have equally important implications for the new demands of public health, including disease reporting and social contract tracing.

The effectiveness of the new regulations – and the success of the nation's simultaneous efforts to combat COVID-19 – will depend on how well individual healthcare organizations collect, govern, share, and secure their patient data, says Daniel Cidon, Chief Technology Officer for NextGate.

Providers will need complete visibility into their patient populations in order to provide resources to COVID-positive individuals, track infection patterns, and report on outcomes – all while managing the heightened data accountability expectations baked into the industry's new patient data access framework.

Navigating Uncharted Data Management Territory Safely and Proactively

For many providers, enterprise master patient indexes (EMPIs) will be critical for balancing the need for a private and secure digital environment with the unprecedented challenges of COVID-19, Cidon says.

"An EMPI provides a scaffolding for good data governance so organizations can provide the right care to the right individuals while safeguarding those individuals' information," he said. "As we start adjusting to COVID-19, and especially as we start to develop contact tracing programs to control the spread of the virus, reliable patient matching and strong data governance are going to be even more important."

Proactive management of the pandemic will require contact tracing agencies to identify all the places a person has been and all the other people that individual has come into contact with. While experts will likely need to spend more time hashing out the ethical and legal boundaries of contact tracing programs, healthcare providers will have to be prepared to supply the necessary data when asked, Cidon said.

"Reliable patient identity management is very important for identifying groups of people who may be related to each other or share a household," he explained. "We can see who shares a doctor and who may have been exposed during an office visit. And in addition to controlling spread at a community level, we can use that information to match people to services they may need if they are showing symptoms or test positive for the virus."

EMPIs can be a major component of recovery because EMPIs synthesize so much information from so many different sources and help create trustworthy profiles for individuals.

"If we review lab feeds, for example, and see a positive COVID-19 test, we may be able to surface that information to the right providers to make sure that person gets support and follow-up," he said.

However, not all EMPIs are created equal, Cidon cautioned, and not all platforms will adequately support healthcare organizations as the industry moves into uncharted data management territory.

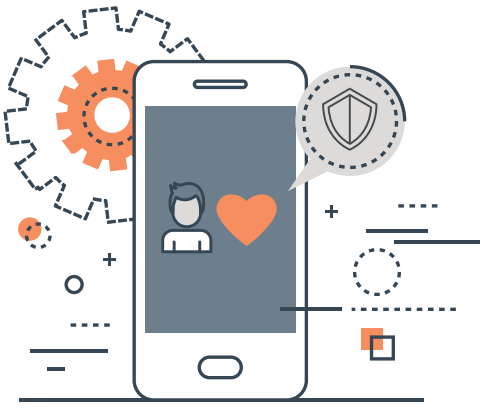
"Organizations have to make sure they are employing the right strategies to balance privacy with public health, including being fully aware of where data is moving, who has access to sensitive data elements, and how patient information is being used," he stressed.

"Privacy must continue to be a top priority for healthcare organizations going forward. Privacy starts with accountability. And accountability starts with having visibility and appropriate control over who is accessing data and how they are using it."

Organizations will need to assess their data governance processes to ensure they have the right controls and permissions in place to safeguard data without running afoul of data sharing and reporting requirements.

"Healthcare providers are going to be held accountable to that – they're going to be held to the highest standard, whether by regulators, by local public health authorities, or by their patients," Cidon said. "As a provider, your EMPI strategy must help you meet your data governance responsibilities without exposing you or your patients to risk."

Taking ownership of data governance to meet modern privacy needs



The famous data science maxim "garbage in, garbage out" applies to patient identity management just as much as anywhere else in the health IT environment, Cidon says.

"Your patient matching and your unique identifiers are only going to be as good as your data capture workflow," he stated. "If your organization isn't taking ownership over the processes of ensuring complete and accurate capture of patient data at the point of service, there is no EMPI in the world that will be able to perform perfectly against poor data."

"One of the most frustrating things we see from healthcare organizations is the expectation that they can simply throw their data over the wall to an EMPI vendor and expect the vendor to handle everything," he continued. "Some vendors do promise that, but it's not something they can realistically follow through on."

EMPIs are typically organized around one of two major models, he explained. The first focuses on establishing strong internal data governance processes from the beginning to the end of a data element's lifestyle, creating an environment that fosters accurate patient data matching, avoids duplicate patient profiles, and allows data to stay local to the organization where it originated.

The second model relies more on data aggregation techniques and the probability that a patient's true identity can be assembled from among a huge pool of potentially relevant data elements. The EMPI vendor largely takes on the responsibility of combing through the melting pot of data to ensure patient profiles are complete and accurate.

"On the surface, that type of large-scale data aggregation looks very attractive to healthcare organizations, in part because it seems a lot simpler than having to be meticulous about managing their own data," acknowledged Cidon. "But there are a lot of pitfalls with this approach."

> Healthcare organizations that agree to add their data assets to a third-party stockpile risk relinquishing critical control over that information.

First, there is the basic concern about hoarding hundreds of millions of pieces of sensitive data in a single location, making it more susceptible to a highly damaging data breach. In 2019, data breaches cost healthcare organizations more than $4 billion, with an estimated cost of $423 per record, found a recent report from Black Book Market Research.[2]

Second, healthcare organizations that agree to add their data assets to a third-party stockpile risk relinquishing critical control over the use and reuse of that information, Cidon stressed.

"Your data can be used for a variety of different purposes, some of which are for the vendor's benefit and not yours," he said. "We have seen so many recent cases outside of the healthcare industry where data is being used for inappropriate reasons, and there's no reason to think our industry is going to be exempt. Exposing your patients to that risk is not necessarily a good business decision."

Aggregating data under a third party's control also puts sensitive clinical information at greater risk, he added.

"How can you be sure that you are maintaining separation between certain data, such as behavioral health data or HIV/AIDS status, and the clinicians who don't necessarily need access to it? What happens if that information is accidentally exposed during a contact tracing activity to the wrong entity?"

"You simply cannot afford to lose strict control over privacy and consent models for those types of elements. In addition to the tangible penalties for that type of mistake, the toll it takes on an organization's reputation is incalculable."

Making informed, justifiable decisions around patient identity management

Appropriate data access and use is especially important in light of the new CMS data access rules and ONC interoperability rules, which require healthcare organizations to be able to provide access to information at a patient's request – or justify their decision-making process when data is not accessible for any reason.

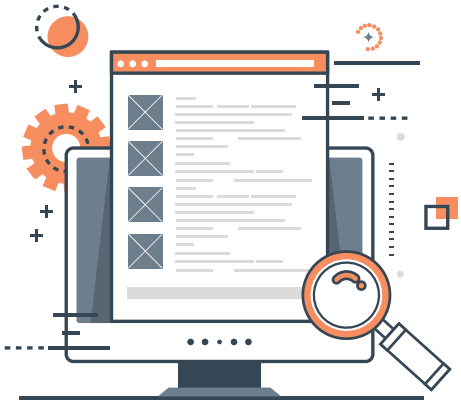
In the Cures Act final rule, the ONC established guidelines around information blocking that come with certain exceptions, such as the infeasibility of a request or the need to protect a patient's privacy.[3] But healthcare organizations cannot use these exceptions as blanket excuses for withholding certain data. Nor can they afford to lose sight of meaningful controls on keeping personally identifiable information private and secure.

"In the context of these rules, we talk a lot about how some organizations withhold information, purposely or otherwise," said Cidon. "But we also have to remember not to minimize the impact of the flip side."

"Patients want more control over how their data is being used and who has access to it. These rules reinforce their right to that control. If you can't answer questions about how a patient's phone number is being used, for example, you might be in a bit of a sticky situation, especially as we start to dive into some of the very thorny privacy issues that will be part of COVID-19."

Local management of patient identities with limited and controlled use of external data sources allows for more accountability because providers retain visibility into which systems contributed to a patient's identity profile, as well as when those decisions were made, what was updated when, and why two records were linked together.

The intersection of these enhanced regulatory requirements with the growing pressures of COVID-19 will create a complex environment for healthcare organizations already coping with numerous changes to the way they operate every day.



No matter what the next challenge, patient privacy and data governance will need to be a key part of the solution, Cidon said.

"Ultimately, it doesn't really matter if you're trying to prevent duplicate records, meet a patient's expectations for data sharing, or trace COVID-19 exposure patterns: privacy is going to continue to be a considerable concern for healthcare organizations and patients," he said.

"It's going to be especially important to be able to justify your data governance decisions in the months or years ahead so I would recommend having a very detailed conversation with a potential EMPI partner to discuss these issues before you agree to a working relationship. Make sure you know what is happening with the data every step of the way so that you can feel comfortable with the decisions you're making with one of your organization's most important and valuable assets."

HEALTHCARE'S BEST APPROACH

For two decades, NextGate has been helping organizations transform their siloed systems into a seamless, secure and highly efficient network, where individuals are accurately and consistently matched to their data. Our identity matching solutions connect the entire healthcare ecosystem into a single, fully integrated view to drive critical improvements in quality, efficiency and safety.

NextGate's flagship enterprise master patient index (EMPI) currently manages patient identities for more than two-thirds of the U.S. population and a third of the population in the U.K.

To learn more about NextGate's market-leading identity management solutions, visit nextgate.com.

References

1. HHS Finalizes Historic Rules to Provide Patients More Control of Their Health Data, Health and Human Services, March 2020 https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html#:~:text=The%20ONC%20final%20rule%20updat.

2. Healthcare Data Breaches Costs Industry $4 Billion by Year's End, 2020 Will Be Worse, Black Book Survey, November 4, 2019, https://www.prnewswire.com/news-releases/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-will-be-worse-reports-new-black-book-survey-300950388.htmll.

3. ONC Cures Act Final Rule, Information Blocking, https://www.healthit.gov/curesrule/final-rule-policy/information-blocking.

With over 200 customers in nine countries, NextGate is the global leader in healthcare enterprise identification. Committed to helping organizations overcome the clinical, operational and financial challenges that result from duplicate records and disparate data, our full suite of identity matching solutions connects the entire healthcare ecosystem to drive critical improvements in quality, efficiency and safety. NextGate's market-leading EMPI currently manages 350 million lives and is deployed by the nation's most successful healthcare systems and health information exchanges.

To learn more, please visit **www.nextgate.com**.

NextGate Solutions, Inc.
3579 E. Foothill Blvd.
Suite 587
Pasadena, CA 91107

aws partner network

Microsoft
One Commercial Partner

Recognized by Gartner as a 2019 Next-Generation EMPI Vendor.
Gartner®