Health Research Institute

Regulatory Insight

pwc.com/hri

Updated March 2020

At a glance:

A regulatory push by CMS and the Office of the National Coordinator for Health Information Technology aims to shift the way the healthcare system shares data, moving from a system where healthcare organizations may share data under HIPAA to one where they must share data. This has immediate and long-term implications for payers and providers faced with a healthcare infrastructure not built for interoperability

Contacts

Benjamin Isgur, Leader
Health Research Institute (HRI)
benjamin.isgur@pwc.com

Trine Tsouderos, Director
HRI Regulatory Center
trine.k.tsouderos@pwc.com

Crystal Yednak, Senior Manager
HRI Regulatory Center
crystal.yednak@pwc.com

Jaclyn Speer, Analyst
HRI Regulatory Center
jaclyn.n.speer@pwc.com

Beyond IT: Why the regulatory push toward interoperability requires whole organizational responses from providers, payers

In the vision sketched out by Congress and regulatory agencies of an interoperable US health system, data moves freely and securely along with the consumer, with vibrant apps connecting patients and their wearables to care teams. Providers and payers share information immediately and fully with traditional competitors and third-party developers, while information blockers holding up care coordination are shamed from hoarding data.

The result? A full patient picture that empowers the healthcare ecosystem to better identify prevention opportunities, eliminate the cost and frustration of duplicate tests and endless forms to fill out, and enable patient data to move seamlessly between providers, and between health plans.

But this vision collides with a reality where only 31 percent of office-based physicians can integrate electronic health information from other organizations without someone manually re-entering the information, according to a 2018 ONC report to Congress. And it's not clear if providers see sharing data with each other as a priority. In a 2019 PwC Health Research Institute (HRI) survey of provider and payer executives, fewer than 24 percent said data sharing with healthcare providers was a top opportunity to improve the patient experience, ranking below call centers for patients and patient adherence programs.

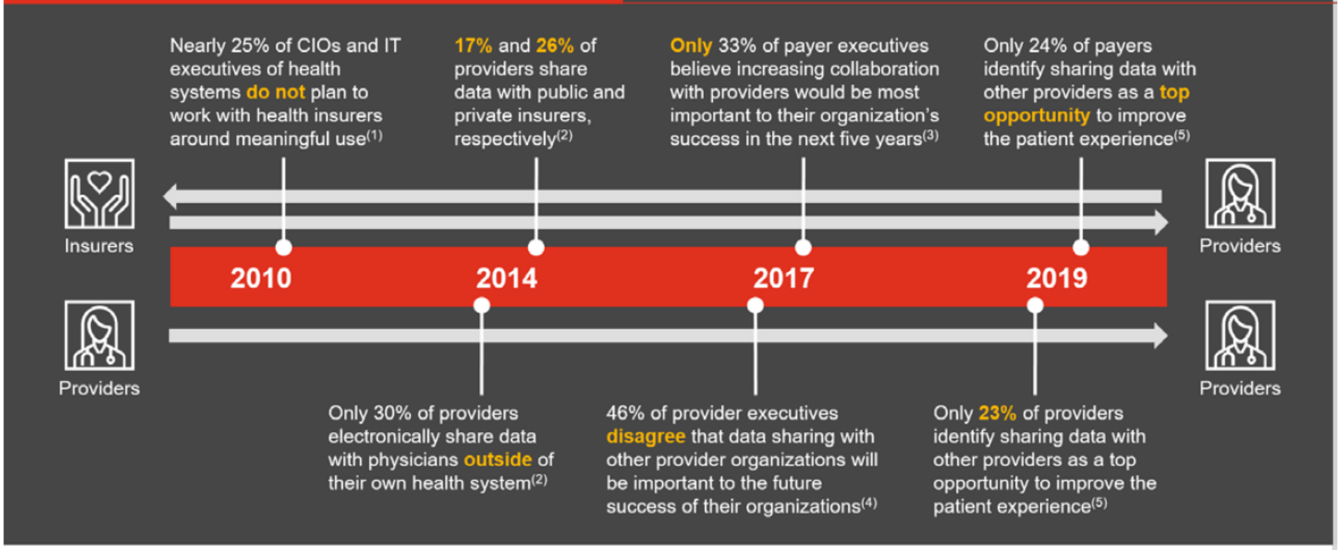
While some leaders in both the payer and provider sectors have embraced data-sharing efforts to craft social determinants of health strategies or strengthen value-based care, the needle has not really moved on providers and payers' attitudes toward data sharing in the past decade, despite industry-led and government campaigns (see Figure 1).

Given the direction of government agencies, healthcare organizations should develop immediate strategies to meet regulatory deadlines, and also consider a longer-term vision of how they may take advantage of enhanced data sharing efforts to strengthen their own outlook.

The promise of retail health, value-based care, improved patient experience and social determinants of health strategies cannot truly be realized without the foundation of an interoperable system in place. “Safe and secure information sharing is critical to improving coordinated patient care, health outcomes and driving value across the entire system,” said Ceci Connolly, president and CEO of the Alliance of Community Health Plans.

Figure 1
Resistant data sharers

Attitudes of providers, payers toward data sharing have not changed much over time



Nearly 25% of CIOs and IT executives of health systems **do not** plan to work with health insurers around meaningful use(1)

17% and **26%** of providers share data with public and private insurers, respectively(2)

Only 33% of payer executives believe increasing collaboration with providers would be most important to their organization's success in the next five years(3)

Only 24% of payers identify sharing data with other providers as a **top opportunity** to improve the patient experience(5)

Only 30% of providers electronically share data with physicians **outside** of their own health system(2)

46% of provider executives **disagree** that data sharing with other provider organizations will be important to the future success of their organizations(4)

Only **23%** of providers identify sharing data with other providers as a top opportunity to improve the patient experience(5)

Sources: (1) 2010 HRI Survey of CHIME CIO Members; (2) 2014 HRI Clinician Workforce Survey; (3) 2017 HRI Payer Executives Survey; (4) 2017 HRI Provider Executives Survey; (5) 2019 HRI Cross Sector Survey

And the drive to make patient health information more available through apps could fuel new entrants seeking to capitalize on a freer flow of data, leaving behind the companies that collected that data in the first place.

"Interoperability is viewed as a 'technology' issue, but this will transform how we operate in healthcare," said Lauren Riplinger, vice president of policy and government affairs for the American Health Information Management Association.

The final rules will require new processes, workflows, investments and partnerships depending on where the organization sits in the healthcare ecosystem. Healthcare organizations should look to build proactive, rather than reactive, strategies to succeed.

In line with the 21st Century Cures Act, HHS' final regulations require CMS-regulated payers, such as those in Medicare Advantage, Medicaid and CHIP Fee-For-Service and managed care, as well as some qualified health plans in the federal exchanges, to make patient claim, encounter, cost and some clinical data available to beneficiaries using an application programming interface (API) based on Fast Healthcare Interoperability Resources (FHIR). Industry-developed, FHIR presents a standard for exchanging data between healthcare applications. The agencies foresee payers sharing patient information with each other as patients move from plan to plan. For their part, providers would send notifications to other providers as patients are admitted, discharged or transferred. And basically, anyone certified in health information technology would have to use an application programming interface in their system that makes patient data accessible in a more meaningful format, such as mobile or web-based app.

In a world that can create financial systems where consumers can access sensitive financial data from nearly anywhere and extract their own cash in moments, why hasn't healthcare been able to achieve a similar result? The effort to incentivize providers into "meaningful use" of their electronic health records systems did result in most providers adopting electronic health records, but a 2017 HRI report on EHRs in the New Health Economy found it did not provide a foundation for true interoperability of those systems.

"All these entities spend hundreds of millions of dollars to put in these EHRs but the ability to actually provide care coordination is limited primarily because patients go to more than one delivery system," said Dr. David Chin, distinguished scholar with Johns Hopkins Bloomberg School of Public Health who specializes in value-based care. "Everyone wanted to create a walled garden so to speak."

Provider executives concede as much, with 68 percent saying they implemented electronic health records to comply with meaningful use requirements over addressing broader business strategy, according to HRI's 2017 provider executive survey. Roughly half said their electronic health record system was used for provider-to-patient communication. About 35 percent said it was used for care coordination, and 30 percent for communications with other providers.

"Once you have that individual inside your system, you have no incentive, and are strongly resistant, to letting them part. Part of the reason why we've seen information silos in healthcare is a bit around this desire to sustain a relationship with a given individual across an enterprise," said Lee Shapiro, co-founder and managing partner for 7Wire Ventures, a healthcare venture fund focused on entrepreneurs working to create informed and connected health consumers. "A (car) dealer isn't going to share their data with the (competing car) dealer up the street."

Payer executives seemed slightly more open, with 72 percent saying when surveyed by HRI in 2017 that they were working on collecting, analyzing and disseminating data to providers to help better coordinate care. Payers have been able to participate in CMS' Blue Button 2.0 program that was rolled out for Medicare Fee-For-Service (FFS) in 2018, allowing beneficiaries to access their health claims information electronically through the application of their choosing. By December 2019, 51 apps had been developed for Medicare beneficiaries through Blue Button 2.0, up from 18 in February, according to CMS data. But the Blue Button 2.0 experience also has brought to life some of the concerns organizations have about expanded data sharing, as CMS on Dec. 4, 2019, had to close down access to Blue Button 2.0 after a bug was discovered that may have caused certain protected health information to be shared with other beneficiaries or the wrong Blue Button 2.0 application. It was restored on Dec. 27, according to CMS.

Some smaller health plans may not have the workforce or the data operations to pivot easily to interoperability, as health plan claims databases were built for reimbursement purposes, not to serve as medical record systems.

Organizations may need to rethink processes to accommodate the shift to a more interoperable health ecosystem. Will payers be able to receive requests to transfer patient information to another payer and be able to provide the required data that meets the US Core Data for Interoperability standard? And, with the use of APIs, organizations will need to establish and prove the identity of the patient who is asking to connect directly into their systems and authenticate the patient app to the electronic health record and other systems. Complying with the rules will likely require a whole organizational response and reallocation of resources, which could interfere with other strategic priorities.

Third parties present a murky situation

The introduction of third-party app developers or digital health companies raises concerns around protection of patient data. While healthcare entities are acting to protect health information under the 1996 Health Insurance Portability and Accountability Act (HIPAA), consumer app developers are not necessarily covered by that law and related regulations. "The real challenge on the privacy side is patients may not immediately understand that when their information leaves the electronic health record and enters a third-party app, that information is no longer HIPAA-protected," said Samantha Burch, director of health IT policy for the American Hospital Association. "I work in this space and I don't generally read every word of an app's terms and conditions. What we're talking about is not how many steps you took today — we're talking about people's most sensitive information, so I think that will create a pretty big learning curve."

The HHS Office of Civil Rights issued guidance in April to clarify the HIPAA-related responsibilities in sharing data with third-party apps, with the agency stating "once protected health information has been shared with a third-party app, as directed by the individual, the HIPAA covered entity will not be liable under HIPAA for subsequent use or disclosure of electronic protected health information, provided the app developer is not itself a business associate of a covered entity or other business associate." This puts the onus on the patient to understand that the application they select may not provide adequate security protections.

The final rules allow payers and providers to educate consumers on their websites and elsewhere of the potential risks of data transfers with third parties outside of HIPAA. They can caution consumers to be sure they understand any secondary data use policies the app may have. But "such efforts generally must stop at education and awareness or advice regarding concerns related to a specific app," the rule states.

Healthcare organizations still have an interest in protecting both their relationships with consumers and their reputations. This raises questions of when, where and how payers and providers are to properly educate patients and inform them of the risks of sharing their data. It's not clear that consumers would make the legal distinction about a provider or payer's role should patients find their sensitive health information misused.

Industry groups also are trying to develop consensus for how third parties will use, store and manage consumer health data to prevent it from being used for other purposes, such as marketing or even being sold, without their consent. The CARIN Alliance, a nonpartisan organization that brings together payers, providers, pharma, technology companies and consumer groups, has drafted a code of conduct for companies handling health data outside of HIPAA to make sure consumers can consent to how it is used.

Business associate agreements may need review or to be extended to more entities. Although tech company business associate agreements that provide access to consumer health data are not unheard of, news reports about large tech companies gaining access to health system data to try to develop insights and tools has provoked consumer uproar and renewed interest in Congress to revisit the issue of health data privacy, which could collide with CMS' push to force data sharing.

A roadblock to an interoperable system has been the incentives providers and payers had to block others from obtaining their data for fear competitors would steal their consumer base or new entrants could figure out how to pull the value from the data. "Obviously hospitals are using data for increasingly advanced analytics to improve population health and risk management and address many other issues, but yes, I think that [the entrance of third-party apps] does create a concern about potential misuse of patient data for commercial purposes," said Samantha Burch of the American Hospital Association.

But the practice of "information blocking" — in which healthcare organizations either refuse to make a patient's data available to others serving the patient, or they have inherent technological impediments — has inhibited a true interconnected system. "I'm sympathetic to information blocking concerns and privacy issues, but I also see people in the marketplace who won't share their data," said David Horrocks, president and CEO of the Chesapeake Regional Information System for our Patients (CRISP). "I think it's worth trying to break the logjam here. I would be shocked if the enforcement was taken against people who were making good faith efforts to behave appropriately."

HRI research has shown that together, payers and providers can develop a more accurate view of the patient that can help improve the patient care experience (see Figure 2). For their part, consumers appear open to healthcare providers sharing their electronic health record with other providers, with 68 percent indicating they were comfortable with it in HRI's 2019 survey of American consumers.

If patients can walk into their preferred venue with their entire medical history, the care venue choice becomes more fluid, more personal and more convenient. Patients benefit from not being asked for the same information multiple times or being subject to multiple versions of the same test because one location does not have access to a previous result.

Questions remain in the industry about how much patients themselves want to interact with their data and if they will use it to change behaviors or make health decisions. In 2018, roughly 3 in 10 individuals were offered access to their online medical record, and also viewed their record at least once within the past year, according to a May 2019 data brief from the Office of the National Coordinator for Health Information Technology. Of those who didn't view their record, a top reason was wanting to speak to their provider directly.

"Just putting information into the ether is not going to empower consumers. Is the information consumable to them? Can they derive value from it?" said Stephanie Cook, chief compliance officer for Dean Health Plan and WellFirst Health. Dean Health Plan provides coverage to more than 400,000 members in southern Wisconsin, and WellFirst Health is new to the St. Louis market in 2020. Both are part of SSM Health, a St. Louis-based integrated health system. "Our concern is we are going to be opening every system to make available all the information we hold," Cook said.

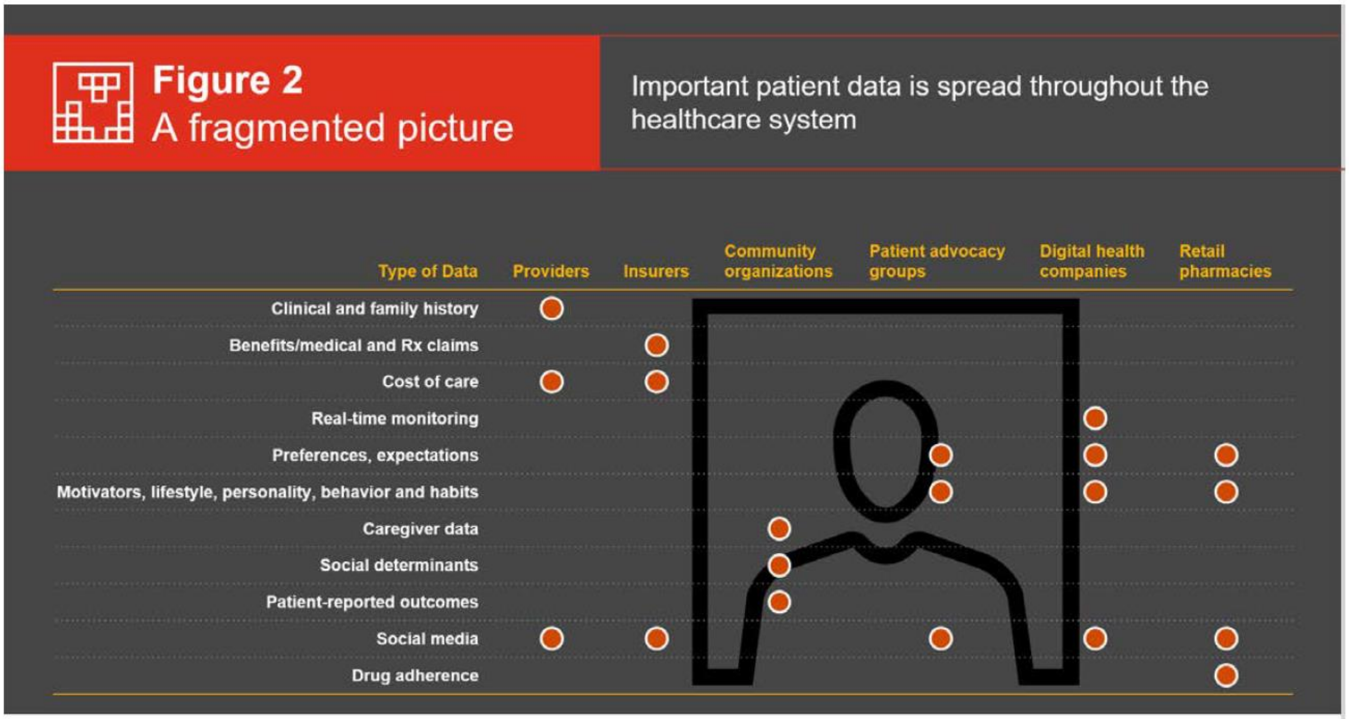


Figure 2
A fragmented picture

Important patient data is spread throughout the healthcare system

Type of Data	Providers	Insurers	Community organizations	Patient advocacy groups	Digital health companies	Retail pharmacies
Clinical and family history	●					
Benefits/medical and Rx claims		●				
Cost of care	●	●				
Real-time monitoring					●	
Preferences, expectations				●	●	●
Motivators, lifestyle, personality, behavior and habits				●	●	●
Caregiver data			●			
Social determinants			●			
Patient-reported outcomes			●			
Social media	●	●		●	●	●
Drug adherence						●

Source: PwC Health Research Institute,"Consumer Experience in the New Health Economy: The data cure," 2018.

"How's it going to be used? It's vital we ensure our members' protected health information is kept safe in this new environment."

Technology companies are betting that consumers do want the data access, and some are interjecting themselves into the picture to take the information and help make it more usable for patients.

In November 2019, the Veterans Health Administration announced that veterans who are iOS users could access their patient records through the Apple Health app on their phone, an initiative made possible through the Veterans Health API. A more robust exchange of patient data could help efforts to solve for the social determinants of health, the social, economic and environmental factors that can have a bigger influence on health than clinical care.

By combining data from throughout the healthcare system and community organizations, providers and payers can identify the behaviors and social challenges impacting health and develop intervention strategies to target those social determinants of health in powerful ways that have yet to be fully explored. They could also use the insights they glean from the patient's full record to take advantage of outcomes-based payment structures.

"Having interoperability in place can be an accelerator because you're spending less time, energy and investment on creating the data exchange pathways, and can rely on this underlying infrastructure to focus more on structuring the focus areas and ecosystem incentives to make sure the members are getting the right care at the right time in meaningful ways," said Himanshu Arora, chief data and analytics officer for Blue Cross Blue Shield of Massachusetts. "That's the next step to making value-based care even more real, and ensuring that the healthcare ecosystem as a whole is able to focus on the triple aim of cost, quality and consumer experience."

Third parties can help bridge the gap for health organizations that are not in the position to make the data usable and understandable. "That's where innovation comes in on top of providing this raw data," said Lee Shapiro of 7Wire Ventures, who is also chief financial officer for Livongo, an applied health signals company that uses data to help people manage chronic disease. "I do think that part of this data is going to create a new canvas for innovation to paint on. So we have some really great opportunities here, but this has to evolve."

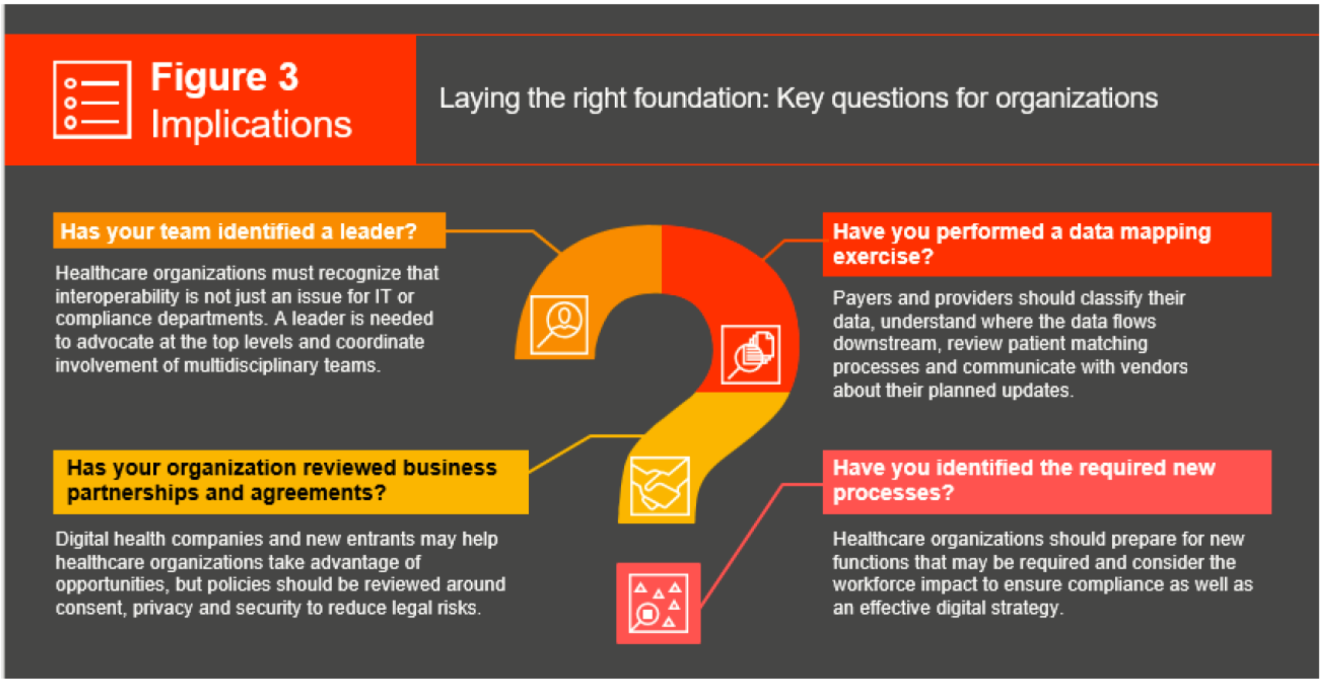


Figure 3
Implications

Laying the right foundation: Key questions for organizations

Has your team identified a leader?

Healthcare organizations must recognize that interoperability is not just an issue for IT or compliance departments. A leader is needed to advocate at the top levels and coordinate involvement of multidisciplinary teams.

Have you performed a data mapping exercise?

Payers and providers should classify their data, understand where the data flows downstream, review patient matching processes and communicate with vendors about their planned updates.

Has your organization reviewed business partnerships and agreements?

Digital health companies and new entrants may help healthcare organizations take advantage of opportunities, but policies should be reviewed around consent, privacy and security to reduce legal risks.

Have you identified the required new processes?

Healthcare organizations should prepare for new functions that may be required and consider the workforce impact to ensure compliance as well as an effective digital strategy.

Implications

Identify a leader.

This is not just an issue for IT or compliance departments; this demands a cultural and technological shift in healthcare as it moves the system from one where organizations may share data to one where they must share data. A leader is needed within payer and provider organizations who can advocate at the top levels and coordinate involvement of multidisciplinary teams. Compliance deadlines for certain provisions that require new operations could pose a tight timeline for some companies.

In some organizations this may be a chief data or digital officer who can spearhead the organization's response. Others may determine it's everyone's role in the organization to think digitally.

Leadership is needed across sectors as well. "Stakeholders nationwide must come together to move us toward a fully interoperable system – health plans cannot do it alone," said Ceci Connolly of the Alliance of Community Health Plans.

Map out your data to see what's affected.

Payers and providers should assess the state of their data and consider what unstructured data sets exist. They should classify the data to understand which may contain personal health information targeted by new regulations and where the data flows downstream. Data cleanup efforts and an assessment of how much of the data conforms to industry standards are also important, along with a map of who controls the data, when it is pushed out and to whom.

In the absence of a single, unique patient identifier in the US, healthcare entities have long struggled to match patients when different identifiers are used by other organizations with whom they exchange data. The industry has been working on this problem for many years and it may still present a serious impediment to data exchange as well as a serious patient safety risk. Now is also a good time to review patient matching processes and develop different methods for crosswalking patient identifiers or demographic information. Interoperability efforts that multiply the number and complexity of data exchanges heighten the importance of accurate patient matching processes.

Providers should communicate with vendors about what updates they may have planned for EHR systems to respond to the regulations. But organizations should not look to one vendor to entirely solve the challenges of the new rules, as a successful response will require technical, procedural and administrative changes throughout the organization.

Review business partnerships in this new regulatory environment.

Digital health companies and new entrants may help organizations take advantage of the opportunities that achieving interoperability may present. However, the freer flow of information opens up new questions about data privacy, as some companies accessing the data may not be covered under HIPAA.

Companies should consider the legal risks and take steps to protect their reputations and relationships with customers by thinking through issues of consent and data privacy. Healthcare organizations should review their current policies and consider whether they offer protections for customers under the new processes and what data security risks may emerge. They should also consider whether business associate agreements are due in more situations.

Prepare for new processes.

Healthcare organizations may find that they have entirely new functions to perform that they've not performed before, such as notifying other providers of a discharge or making patient data available via API.

Providers and payers should consider not only potential cost implications and new workflows, but also the impact to workforces and the training that will be needed to ensure not only compliance but an effective digital strategy.

Acknowledgments

Himanshu Arora
Chief Data and Analytics Officer
Blue Cross Blue Shield of Massachusetts

Samantha Burch
Director, Health IT Policy
American Hospital Association

Dr. David Chin
Distinguished Scholar
Johns Hopkins University
Bloomberg School of Public Health

Ceci Connolly
President and CEO
Alliance of Community Health Plans

Stephanie Cook
Chief Compliance Officer
Dean Health Plan and WellFirst Health

David Horrocks
Chief Executive Officer, President
Chesapeake Regional Information System for our Patients

Dr. David Kendrick
Chief Executive Officer
MyHealth Access Network

Lauren Riplinger
Vice President of Policy and Government Affairs
American Health Information Management Association

Lee Shapiro
Co-Founder, Managing Partner
7Wire Ventures

Virginia Whitman
Public Policy Associate
Alliance of Community Health Plans

Health Research Institute Advisory Team

Jamie Gunsior
Principal
jamie.gunsior@pwc.com

Christopher Van Pelt
Principal
chris.vanpelt@pwc.com

Vaughn Kauffman
Principal
vaughn.a.kauffman@pwc.com

Robert Fassett
Managing Director
robert.t.fassett@pwc.com

Matthew Lawson
Principal
matthew.d.lawson@pwc.com

Lisa Gallagher
Managing Director
lisa.a.gallagher@pwc.com

William Perry
Principal
william.perry@pwc.com

Derek Gaasch
Director
derek.gaasch@pwc.com

John Rich
Principal
john.rich@pwc.com

James Lin
Director
jam.lin@pwc.com