IBM Institute for Business Value | Expert Insights

The urgency of healthcare interoperability

Innovating with shared health data

Experts on this topic

Ryan Hodgin

IT Executive
US Healthcare Organization
linkedin.com/in/rhodgin

Ryan has more than 20 years of experience working in technology and has spent the last 8 years focused on the healthcare and life sciences industry. He is passionate about leveraging technology to improve patient and clinician experiences. Ryan was formerly the IBM Global Healthcare and Life Sciences CTO, where he provided deep technical expertise and thought leadership to healthcare organizations worldwide.

Rohit Pandey

Solution and Industry Architect,
Healthcare and Life Sciences
IBM India
rohit.pandey@in.ibm.com
linkedin.com/in/rohit-pandey-8b7094235

Rohit has more than 17 years of experience working in the tech world with 11 years focussed on healthcare. He has extensive knowledge in creating solutions for payers and providers and loves leveraging technology to enhance patient and practitioner life experiences. His interest in technologically driven innovation includes AI, user experience, machine learning, cloud-native design, and data analytics.

Somasundaram Raman

Practice Area Leader and Healthcare SME/
Business Transformation Consultant
IBM India
soma.raman@in.ibm.com
linkedin.com/in/somasundaram-
raman-b5077613

Soma has more than 30 years of IT experience, with 22 years working globally across healthcare and life sciences. He conceptualizes and delivers solutions using the latest technologies, including AI, digital, IoT, blockchain, and electronic and personal health records. Soma is passionate about leveraging state-of-the-art technologies, improving patient outcomes, and moving from “sick” care to “health” care.

Jeff Wright

Enterprise Architect
Merative
linkedin.com/in/jwright

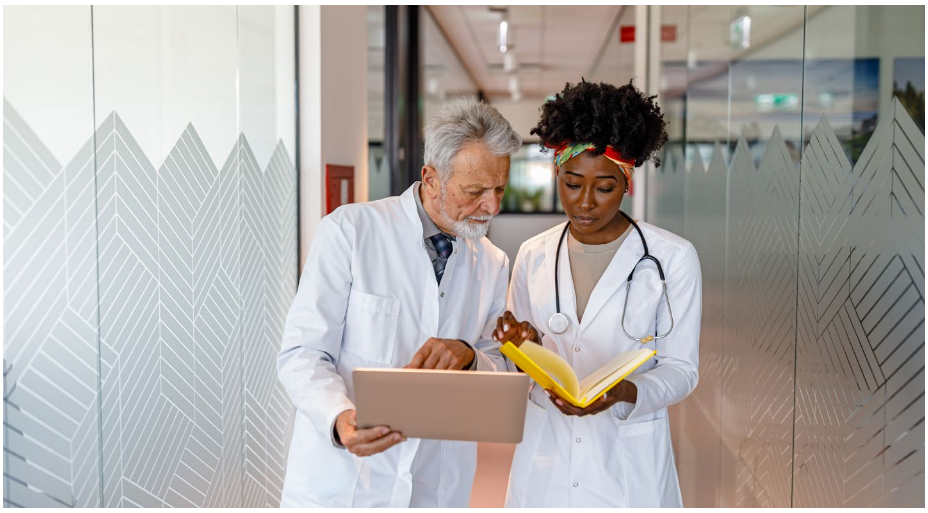
Jeff Wright is an enterprise architect at Merative, where he is responsible for population health analytic products. He has more than two decades of experience creating data-intensive solutions for payers, providers, life sciences, and other industries. Jeffs’ interests include machine learning, cloud-native design, and data architecture.

Executive summary

Healthcare organizations can benefit from breaking down the barriers that currently divide the global healthcare ecosystem. When applications, devices, and systems are able to interact and exchange information in real time, organizations can operate more efficiently—and patients can receive personalized care wherever they go.

In addition, when organizations use open standards, they can share applications and data with reduced friction, transaction costs, and risks. This enables innovative solutions that rely on collaboration—and have the potential to revolutionize the healthcare sector.

Zero trust security is a pathway to this kind of openness. As healthcare organizations become more connected, they need to adopt a holistic cybersecurity model that goes beyond perimeter-based controls, assumes breaches have occurred, and always verifies. The robustness of zero trust can ultimately be the most efficient way to facilitate trustworthy data exchange.



Personalized patient care is possible

We're entering an era of 'precision medicine.'[1] By tapping into the droves of health data individuals generate over a lifetime, healthcare providers are now capable of delivering more customized care across the patient journey.

Smart diagnostic solutions spot patterns that help doctors diagnose illnesses faster and more accurately. Wearable devices let providers remotely monitor patients and deliver better preventative care. And predictive analytics can assess an individual's risk for developing genetic diseases, such as cancer.

As data becomes more accessible across systems, organizations can position themselves to offer more of the personalized healthcare experiences that patients increasingly demand.[2] For example, globally connected health data could empower patients to travel across borders to receive better quality or more affordable care as they see fit.

Connected data promises to improve medical research, as well. If anonymous patient data is shared more openly, scientists can use aggregated information to develop new medications, vaccines, and procedures at a much faster pace. And when new public health threats emerge, hospitals could more easily share data to determine which treatments and protocols would be most effective at scale.

However, most patient data is currently siloed in separate systems, making it difficult for organizations to share information—or even use it internally. That means providers and researchers can only see a small piece of the picture.
To open the aperture, healthcare organizations need to create an ecosystem where applications, devices, and systems can interact and exchange information on demand.

But that's a complicated proposition. Making data sharable and secure requires a new way of thinking about healthcare systems. Rather than each healthcare organization building walls around its own closed system, the industry needs a shared set of rules that govern how patient data can be accessed, exchanged, and stored.

Making data sharable and secure requires a new way of thinking about healthcare systems.

Many governments are already enabling this type of interoperability. For example, by 2025, the European Health Data Space aims to allow citizens across Europe to access their prescriptions and health records online.[3] Yet, global interoperability is still a long way off. Many healthcare systems rely on outdated legacy technology, and some still keep records on paper. In BCG's Digital Acceleration Index, healthcare scored low on the global digital maturity index—eighth place out of nine industries.[4]

At this point, regulatory mandates are driving much of the progress toward interoperability. For example, the No Surprises Act in the US restricts healthcare providers from charging patients more than what their insurance covers for most emergency and some non-emergency services, which used to happen when patients used out-of-network providers.[5] This regulation can increase price transparency for patients—but compliance also requires providers and health plans to share large quantities of data quickly using common standards.

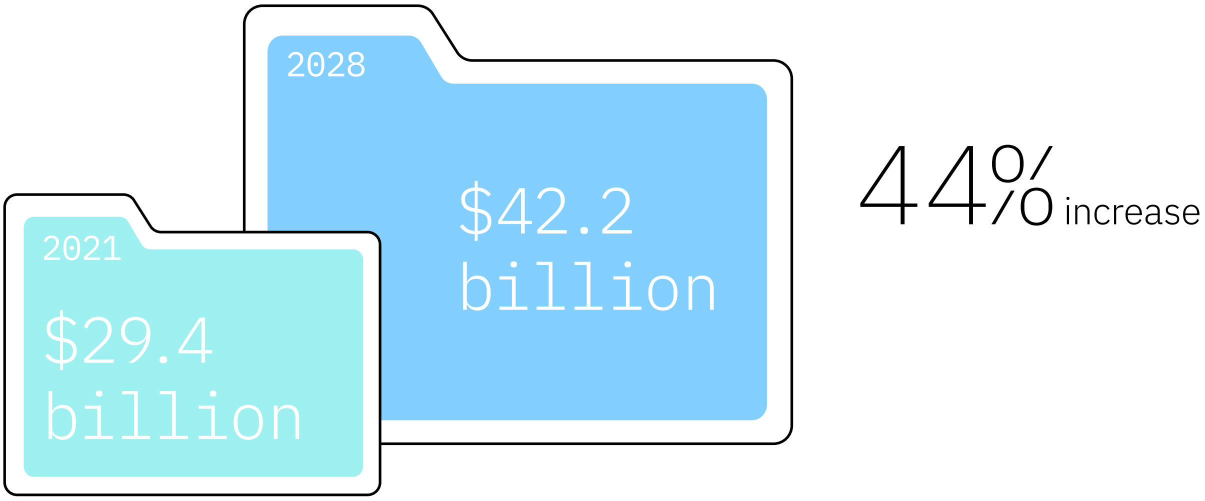
Healthcare providers that look beyond immediate regulatory mandates can also gain competitive and care advantages through interoperability. For example, while the European Commission was spurred to create its digital health exchange by the General Data Protection Regulation (GDPR), the European Commission estimates that, within 10 years, the health exchange could lead to savings of more than €10 billion.[6]

Overall, the opportunity on the horizon is enormous. The global electronic health records market, which was worth $29.4 billion in 2021, is estimated to grow to $42.2 billion by 2028 (See Figure 1).[7] But delivering on this demand requires creating a connected global ecosystem—and supporting interoperability through standards, trust, and openness.

FIGURE 1

Digital demand is on the rise

The global electronic health records market is expected to grow by 44% between 2021 and 2028



Source: "Global Demand of Electronic Health Records (EHR) Market Size & Share to Grow at a CAGR of 6.2%, Expected to Hit USD 42,203.5 Million Mark by 2028." Zion Market Research. May 16, 2022.

Standardization builds bridges

The recent pandemic highlighted how crucial collaboration can be—and healthcare leaders want to be prepared for whatever comes next. The IBM Institute for Business Value (IBV) 2022 CEO Study found that 3 in 4 healthcare provider CEOs cited public health incidents as the number one challenge they expect to face in the next 2 to 3 years (see Figure 2).[8]

However, when each healthcare organization uses its own standards and systems, sharing digital data is inefficient—and far less secure. The Philips Future Health Index 2021 found that difficulties with data management (44%) and lack of interoperability and data standards (37%) present the biggest barriers to adoption of digital health technology in hospitals and healthcare facilities.[9]

That's why open data and transmission standards are at the heart of healthcare interoperability. They help ensure everyone uses the same language and takes the same approach to sharing, storing, and interpreting data. But it's difficult to get organizations across functions, industries, and countries on the same page.

While a global standard for healthcare interoperability doesn't yet exist, many players are working toward one. Government-to-government collaborations, such as The Global Digital Health Partnership, have helped develop a common understanding of challenges, strategy, and standards.[10]

FIGURE 2

Crisis-ready leaders

Healthcare provider CEOs
are focused on future risks

73.6%

cited public health incidents as the top challenge they expect to face in the next 2 to 3 years.

Source: "The 2022 CEO Study. Own your impact: Practical pathways to transformational sustainability." IBM Institute for Business Value. May 2022. Unpublished data.

Countries have started to adopt shared standards in several key areas, including:

- Data format standards, such as Health Level Seven (HL7), which includes Fast Healthcare Interoperability Resources (FHIR) and others; Digital Imaging and Communications in Medicine (DICOM), and Integrating the Healthcare Enterprise (IHE) guidelines
- Data content standards, such as the United States Core Data for Interoperability (USCDI), Systemized Nomenclature of Medicine (SNOMED), International Classification of Diseases (ICD), National Drug Codes (NDCs), and Healthcare Common Procedures Coding System (HCPCS) codes
- Data transmission methods, such as streaming interfaces and representational state transfer application programming interfaces (REST APIs)

Still, each health system has its own rules regarding what data should be captured and how it should be shared. To address individual needs, some countries have created local variations of these standards, such as the Da Vinci and CARIN Blue Button FHIR profile variations in the US.

By creating a common language and a common approach to sharing healthcare data, standards open the door to partnerships that weren't possible before. And broader collaboration can spark game-changing innovations that could reshape the healthcare landscape.

Openness enables innovation

Global healthcare ecosystems are enabled by an open hybrid cloud architecture. This openness lets organizations share applications and data with reduced friction, transaction costs, and risks—whether they're based on the mainframe or in a public or private cloud.

Traditionally, healthcare providers have purchased systems that perform individual functions and are built by individual vendors. Now many struggle with data silos that can't be accessed by partners, regulatory agencies, or even other internal departments. Breaking down those silos promises to unleash new solutions that make precision medicine possible.

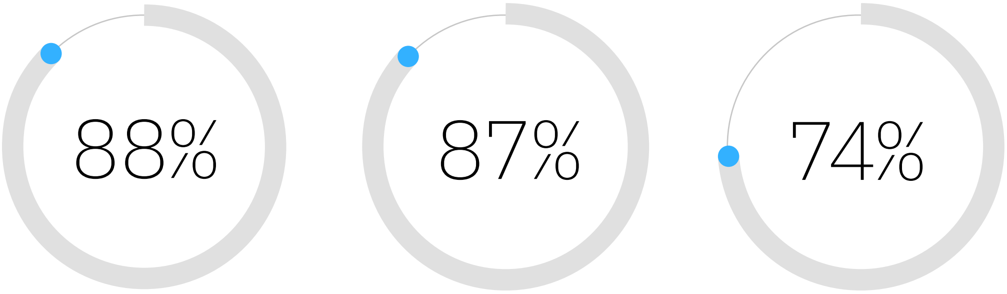
In Estonia, for example, a clinical decision support system helps providers make better decisions using private health data. It analyzes a patient's past diagnoses, medications, recent test results, blood pressure readings, and lifestyle indicators to suggest targeted tests or treatments. The system also helps providers prioritize patients based on the urgency of their condition.[11]

This tool is the first of its kind to be rolled out on a national scale, but it's just the tip of the iceberg. According to Red Hat, 74% of healthcare IT leaders expect the use of enterprise open source for emerging tech to increase in the next 2 years. And nearly 9 in 10 say enterprise open source is as secure as or more secure than proprietary software (see Figure 3).[12]

FIGURE 3

Open source is vital

Healthcare IT leaders say it boosts responsiveness, security, and innovation



Enterprise open source solutions helped address COVID-related challenges.

Open source is as secure as or more secure than proprietary software.

We expect to increase our use of enterprise open source software for emerging technologies.

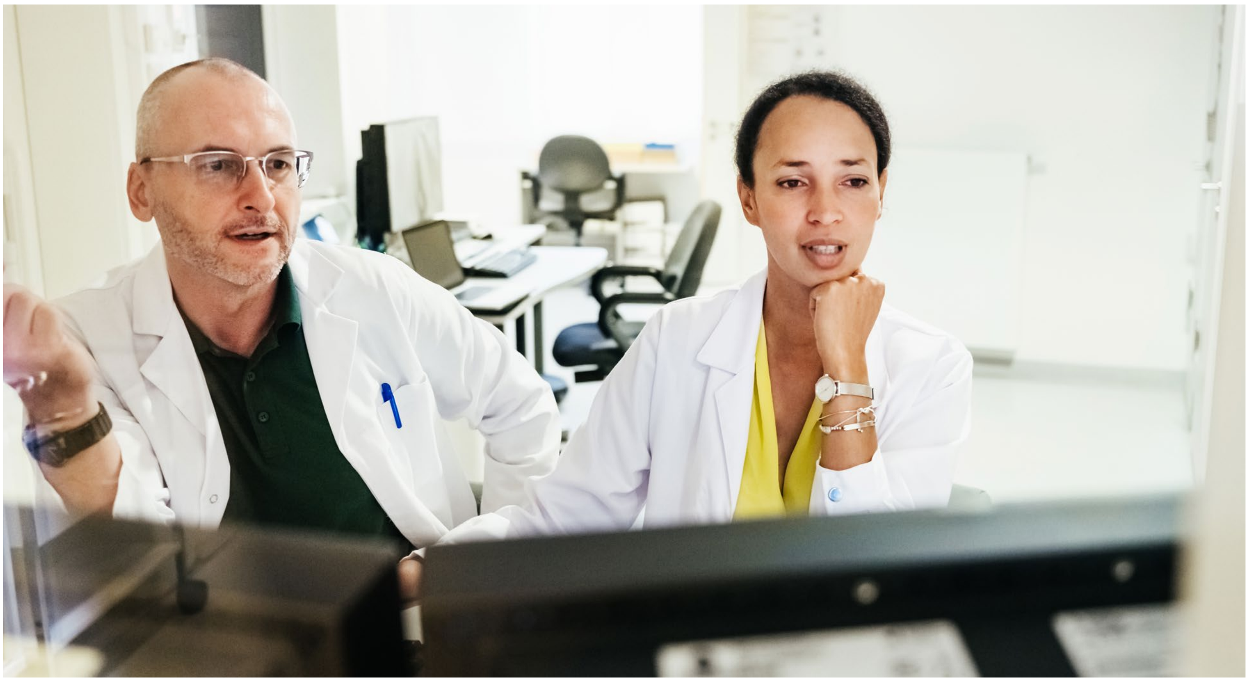
Source: "The State of Enterprise Open Source: Key findings from the healthcare industry." Red Hat. 2022.

This shift to open architecture and open source software is enabling greater collaboration, allowing innovators to develop healthcare applications faster and more cost-effectively. Providers around the world are forming partnerships to launch platforms to share health data and applications.

For instance, 14 health systems recently came together to launch a new startup that aims to improve research and drug development by pooling and analyzing aggregate patient data. The new data platform will use AI and machine learning to help healthcare providers deliver more targeted, personalized care.[13]

Combining platforms and systems in a secure, seamless, and standardized way can help healthcare organizations make a bigger impact at scale. It can break down the walls between different segments of the sector, allowing organizations to address challenges more holistically.

As part of an open ecosystem, healthcare leaders can build partnerships that weren't possible in the past—and find innovative solutions to the world's toughest health problems. But to enable the type of collaboration open innovation requires, all partners need to be confident that the ecosystem is secure.



Security starts with zero trust

In May 2022, a data breach at Choice Health, an independent insurance broker in the US, exposed more than 1.2 million private health records. A database's security settings were misconfigured, which allowed a hacker to download private data—including names, birth dates, and credit card numbers—and offer it for sale.[14]

These types of breaches put patients at risk for identity theft and other types of fraud, and they can be financially devastating for healthcare organizations. While most data breaches are costly, healthcare has had the highest industry cost per breach for 12 consecutive years, according to IBM Security's annual Cost of a Data Breach Report. In 2022, that cost rose to an average of $10.10 million per incident, up from $9.23 million in 2021—and almost double the average of any other industry (see Figure 4).[15]

And as healthcare organizations break down traditional boundaries between systems and organizations, attack surfaces are expected to expand. Protecting patient data in a connected global ecosystem requires a security model that is holistic, multilayered, and event driven. It requires a zero trust approach.[16]

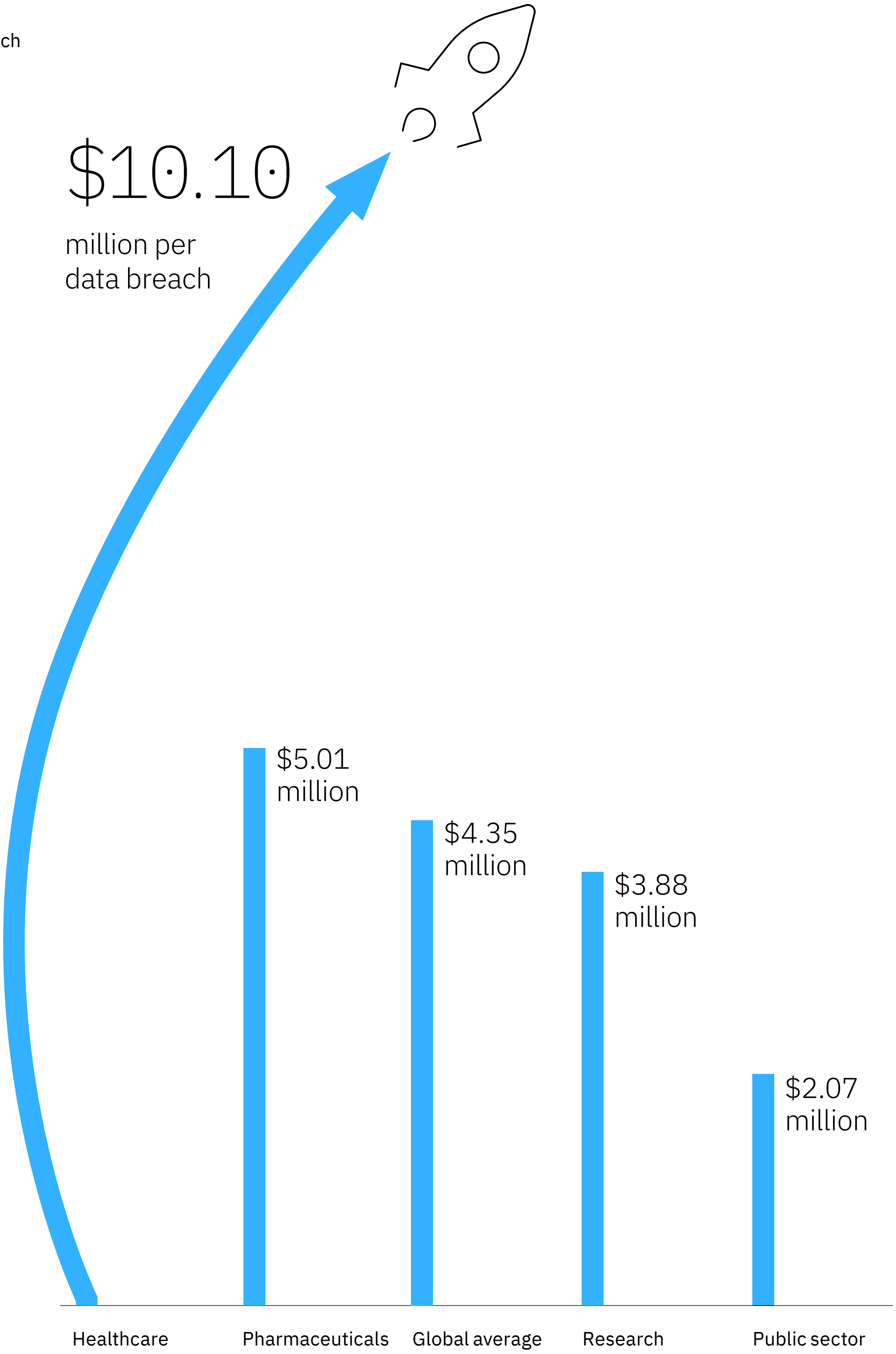
Zero trust is a dynamic framework for cybersecurity that assumes a breach has already occurred. It protects private data by going beyond perimeter-based controls, verifying users through a combination of access controls, identity management, and contextual data.

In 2022, the average cost of a healthcare data breach rose to $10.10 million per incident, up from $9.23 million in 2021—and almost double the average of any other industry.

FIGURE 4

Skyrocketing risk

Healthcare has the highest industry cost per data breach



Source: "Cost of a Data Breach Report 2022." IBM Security and the Ponemon Institute. July 2022.

When organizations assume they're always under attack, they put in robust monitoring and incident response practices that allow them to contain breaches faster. In fact, recent IBV research found that 55% of zero trust leaders were able to prevent malware propagation in the event of the breach, compared with 35% of all other security professionals surveyed. More than half (54%) also said that zero trust has helped them improve network visibility, breach detection, and vulnerability management (see Figure 5).[17]

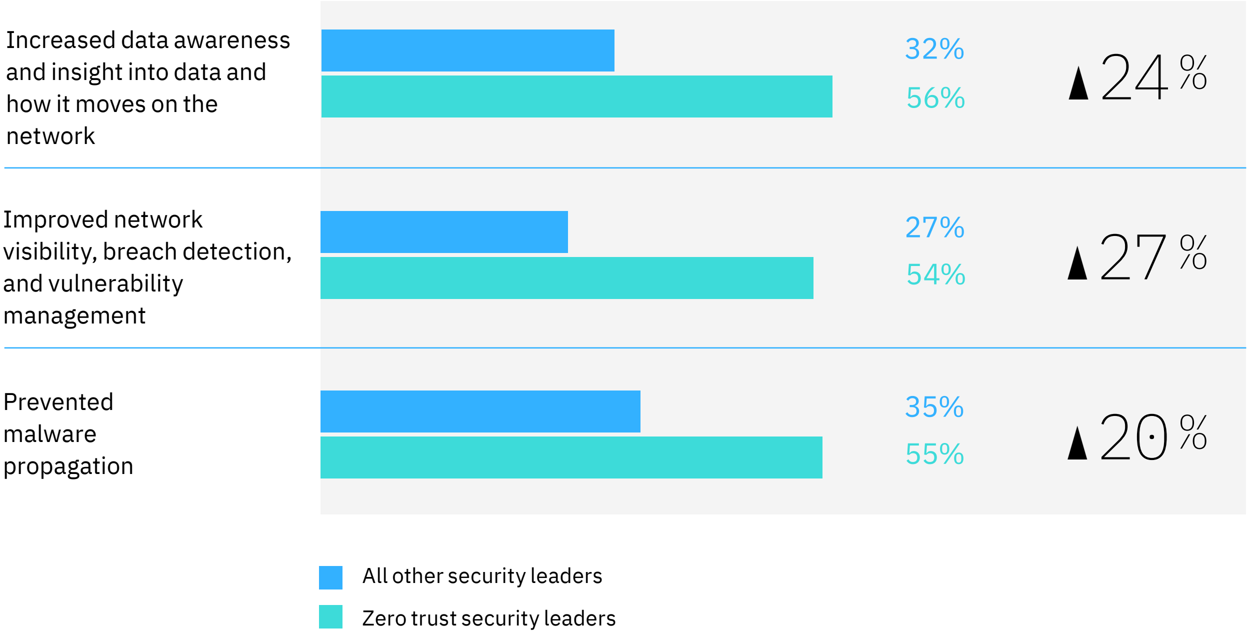
By creating microperimeters around specific assets and services, healthcare organizations can control access to networks and applications, as well as specific data elements. This enhances resilience by helping prevent unauthorized access to data. In fact, IBV research found that 59% of zero trust leaders had successfully prevented the exfiltration of sensitive data, compared with just 34% of all other security professionals.[18]

With zero trust, healthcare organizations can adjust permissions based on circumstance or context, which helps organizations to be more flexible, responsive, and open. And openness facilitates new forms of collaboration and exchanges that, in turn, could revolutionize the healthcare industry.

FIGURE 5

Contain and control

Zero trust security helps organizations detect and address data breaches quickly



Q. To what extent has your organization realized each of the above benefits from its approach to security? Percentages reflect respondents selecting a significant or very great extent.

Source:, "Getting started with zero trust security: A guide for building cyber resilience." IBM Institute for Business Value. July 2021.

Action guide

Connecting the global healthcare ecosystem

A more integrated global healthcare system could help the world tackle the next public health crisis. It could improve patient safety by helping ensure the accuracy of health data and combatting health inequities for underserved populations.

But the path forward will be different for every organization. Targeting a desired solution, such as smart diagnostics, and then working backward can help organizations prioritize the standards, security practices, and architectures they need.

Here are three key actions organizations can take now, regardless of where they choose to start their journey toward interoperability.

01

Align with key standards and adhere as they evolve.

- Be aware of the emerging standards in interoperability, such as FHIR, Trusted Exchange Framework and Common Agreement (TEFCA), and International Patient Summary.
- Agree on key clinical pathways and protocols across organizations.
- Establish consistent methods of identifying individuals and unifying data.
- Define metrics for measuring outcomes and continuously track progress.

Action guide

02

Leverage an architecture that is both open and consistent to spur innovation.

- Leverage cross-industry and healthcare open standards to enable innovation and collaboration, and prevent lock-in.
- Prioritize the use of open source software built by a community of developers and organizations over proprietary options.
- Follow a data fabric model for integrating information across systems and breaking down silos.
- Enable an open ecosystem of partners and vendors to foster innovation and allow for collaboration and competition.
- Integrate operational controls and auditability for consistent management.
- Implement end-to-end security controls, protection of data, and compliance with applicable standards, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Trust Alliance (HITRUST), and GDPR.

03

Approach interoperability in the context of a holistic zero trust security strategy.

- Recognize each party's role and understand the rewards you can achieve through deep collaboration.
- Audit your identity and access management platform to verify that it provides features to secure APIs and support workflows for the lifecycle of onboarding and offboarding interoperability partners.
- Expand your network monitoring and intrusion detection systems to cover all components of your interoperability platform. Automate security operations using tools such as security incident and event management (SIEM) to improve the timeliness and consistency of responses. Establish pervasive encryption on the network and at rest, and ensure that updates and patches are installed quickly.
- Include interoperability in security risk management, security controls, and data loss protection policies. Work with interoperability partners to elevate security controls outside the walls of your business to the health data exchange ecosystem.

About Expert Insights

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based on conversations with leading subject-matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also follow @IBMIBV on Twitter or find us on LinkedIn at https://ibm.co/ibv-linkedin.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

Related Reports

Getting started with zero trust security: A guide for building cyber resilience.

IBM Institute for Business Value. July 2021.
https://ibm.co/zero-trust-security

A hybrid cloud prescription: Accelerating cloud adoption in healthcare and life sciences.

IBM Institute for Business Value. August 2020.
http://ibm.co/cloud-adoption-healthcare

Medical devices are vital, but vulnerable: Treat infrastructure risks to safeguard patient care.

IBM Institute for Business Value. March 2020.
https://ibm.co/medical-device-security

Notes and sources

[1] Hulsen, Tim. “Sharing is Caring—Data Sharing Initiatives in Healthcare.” International Journal of Environmental Research and Public Health. April 27, 2020. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7246891

[2] “75% of U.S. Consumers Wish Their Healthcare Experiences Were More Personalized, Redpoint Global Survey Reveals.” Businesswire. February 18, 2020. https://www.businesswire.com/news/home/20200218005006/en/75-o

[3] Deutsch, Jillian and Lyubov Pronina. “EU Ready to Spend €2.5 Billion on Hub for Health-Care Data.“ Bloomberg. May 3, 2022. https://www.bloomberg.com/news/articles/2022-05-03/eu-ready-to-spend-2-6-billion-on-hub-for-healthcare-data

[4] Horner, Ben, Adina Symreng, Stefano Cazzaniga, Jennifer Clawson, Jaap Schreurs, India Miller, and John Gooch. “Health Care Providers in Europe Need to Boost Digital Momentum.” BCG. June 17, 2021. https://www.bcg.com/publications/2021/digital-adoption-in-european-health-care

[5] Pollitz, Karen. “No Surprises Act Implementation: What to Expect in 2022.” Kaiser Family Foundation. December 10, 2021. https://www.kff.org/health-reform/issue-brief/no-surprises-act-implementation-what-to-expect-in-2022/

[6] De Filippis, Alberto. “Brussels wants to create EU health data space to streamline access.” Euronews. March 5, 2022. https://www.euronews.com/my-europe/2022/05/03/brussels-wants-to-create-eu-health-data-space-to-streamline-access

[7] “Global Demand of Electronic Health Records (EHR) Market Size & Share to Grow at a CAGR of 6.2%, Expected to Hit USD 42,203.5 Million Mark by 2028.” Zion Market Research. May 16, 2022. https://www.prnewswire.com/news-releases/global-demand-of-electronic-health-records-ehr-market-size--share-to-grow-at-a-cagr-of-6-2-expected-to-hit-usd-42-203-5-million-mark-by-2028--ehr-industry-trends-analysis--forecast-report-by-zion-market-research-301548060.html

[8] “The 2022 CEO Study. Own your impact: Practical pathways to transformational sustainability.” IBM Institute for Business Value. May 2022. Unpublished data. Of the 3,000 CEOs interviewed, 5% were healthcare provider CEOs.

[9] “What will the future of digital health look like?” Philips. November 15, 2021. https://www.philips.com/a-w/about/news/archive/features/2021/20211115-what-will-the-future-of-digital-health-look-like.html

[10] “The Global Digital Health Partnership.” HealthIT.gov. Accessed July 12, 2022. https://www.healthit.gov/topic/global-digital-health-partnership

[11] “The best public sector digital service in Estonia is supporting doctors.” E-Estonia. March 17, 2021. https://e-estonia.com/the-best-public-sector-digital-service-in-estonia-is-supporting-doctors/

[12] “The State of Enterprise Open Source: Key findings from the healthcare industry.” Red Hat. 2022. https://www.redhat.com/rhdc/managed-files/ve-eos-key-findings-from-healthcare-industry-infographic-f31145-202202-en_0_0.pdf

[13] Landi, Heather. “Tenet, Providence, other health giants band together to form new health data startup.” Fierce Healthcare. February 16, 2021. https://www.fiercehealthcare.com/tech/tenet-providence-other-health-giants-band-together-to-form-new-health-data-startup

[14] Alder, Steve. “Texas Tech University Health Sciences Center and Baptist Health Report Data Breaches of Over 1.2 Million Records.” HIPAA Journal. June 24, 2022. https://www.hipaajournal.com/almost-1-3-million-patients-of-texas-tech-university-health-sciences-center-affected-by-eye-care-leaders-data-breach/#:~:text=Texas%20Tech%20University%20Health%20Sciences%20Center%20has%20confirmed%20that%20the,record%20vendor%2C%20Eye%20Care%20Leader

[15] “Cost of a Data Breach Report 2022.” IBM Security. July 2022. https://www.ibm.com/security/data-breach

[16] McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security.” IBM Institute for Business Value. July 2021. https://ibm.co/zero-trust-security

[17] Ibid.

[18] Ibid.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | August 2022

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.

IBM®