In collaboration with
the Boston Consulting Group

WORLD
ECONOMIC
FORUM

The Interoperability Challenge of the COVID-19 Return-to-Work App Ecosystem

WHITE PAPER

OCTOBER 2020

COVID-19
#STAYSAFE
#STAYHOME #COVID-19 #STAYSAFE #CORONAVIRUS #CORONA
#STAYHEALTHY #QUARANTINE #SOCIALDISTANCING
9 043 323 LIKES
INFECTION
#CORONAVIRUS
3 504 316 LIKES

Cover: Getty Images/Da-kuk

Inside: Getty Images/Janiecbros

Contents

There is a large and growing app ecosystem to help manage the return-to-work phase of the COVID-19 pandemic – covering everything from contact tracing to self-attestation and lab results. One of the key questions that will need to be answered is how these apps communicate with one another as employees find themselves crossing borders between companies.
This paper lays out the core challenges and current landscape and offers suggestions for companies, governments and NGOs that are participating in this space.

1 Introduction: The interoperability imperative

Key takeaways:

- As companies use technology tools to enable a safe return to work during the pandemic, the growing patchwork of private solutions presents future challenges for employers and employees, and creates potential future limitations.

- Establishing interoperability standards between applications could solve these issues, but interoperability comes with considerable challenges of its own.

As the COVID-19 pandemic shows signs of continuing through 2020 and potentially longer, employers are creating and implementing innovative policies to help their workforces be as productive as possible while keeping workers safe. While working from home has become the norm in many industries, in some businesses or jobs it is not possible. To safely manage staff in the workplace, many employers are turning to technology tools.

These tools perform a range of tasks, often tailored to the needs of a particular business, and evolve as our understanding of the novel coronavirus deepens. Generally speaking, however, these technology tools provide three functions:

1. Automate the employer's permissions framework to grant access to a facility

2. Track individuals on site, both to manage crowding and to record incidences of physical proximity between people

3. Provide exposure notifications to those deemed to have come into contact with a potentially contagious individual

To perform these functions, back-to-work technology solutions require large amounts of sensitive data: identification data, health status data, even location data when on premises. The collection and treatment of such data pose considerable technical and policy concerns, which are exacerbated when the data being collected is from a visitor to a business who is not an employee, or when citizens travel to a different jurisdiction.

At the moment, many employers deal with this complexity by avoiding it: reducing travel altogether and blocking entire classes of individuals from entering their facilities. Other businesses allow people on their premises, but don't collect enough data to ensure a safe environment. The first creates business risk and may not be sustainable; the second creates health risks.

The hypothetical scenarios that follow illustrate the complexity of the data and policy challenges. Technology must perform its three functions (automate entry permissions, tracking, and exposure notification) in different contexts – and each "jurisdiction" (which could be an employer or a government) may employ different technologies and have different policies.

Entry permissions for visitors

FIGURE 1

Scenario: Contractor visits office

Monday
Jean, a contractor, visits your office

Policy
What criteria will YourCo use to grant a visitor permission to enter? Will Jean be tracked around YourCo's facility?

Data and Technology
How will data be collected? How will its integrity be ensured? How will it be stored? Who will have access to the data?

Source: Adapted from data provided by Boston Consulting Group

Suppose a contractor, Jean, visits your office. In order to determine if Jean is safe to enter your facilities, a receptionist may take her temperature and ask a set of questions to try to determine her risk level.

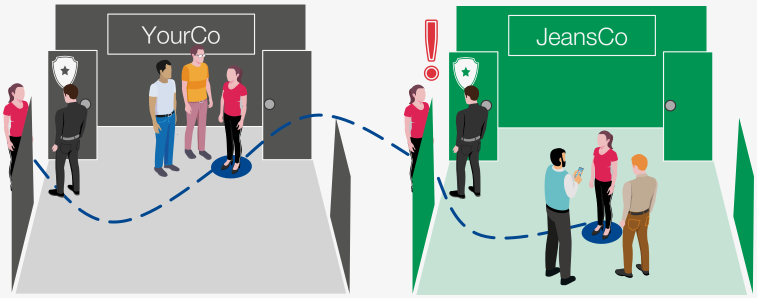
But perhaps Jean's employer has more information about their health, such as a recent negative test result, stored in their own return-to-work application. If that solution were interoperable with your own, that data – or the conclusion that Jean is safe – could be shared.

This would eliminate the need for a manual screen or self-attestation survey as well as improve the confidence in providing permission for the worker to enter the facility.

Entry permissions for staff

FIGURE 2

Scenario: Return to office after a business meeting



Monday
Jean, a contractor, visits your office

Policy
What criteria will YourCo use to grant a visitor permission to enter? Will Jean be tracked around YourCo's facility?

Data and Technology
How will data be collected? How will its integrity be ensured? How will it be stored? Who will have access to the data?

Tuesday
Jean returns to her office

Policy
What information should be used to grant Jean access to her office? How is that complemented by YourCo's information?

Data and Technology
Can JeansCo query YourCos data? How is YourCo's data shared with and verified with JeansCo's system?

Source: Adapted from data provided by Boston Consulting Group

Suppose that Jean wants to return to her office after visiting your office. Is Jean safe to allow back in the building or was she exposed while visiting your office? Your return-to-work information system knows about the COVID-19 status of your employees, and may track their movements for exposure notification purposes while in your facilities.

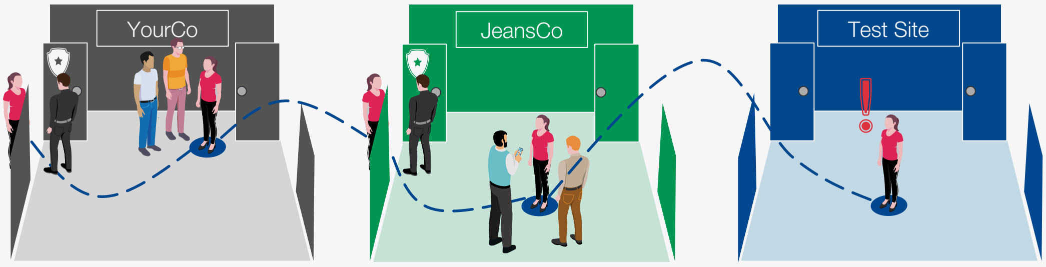
If your company's system is interoperable with Jean's, you could have allowed Jean's proximity to others to be tracked while in your office and then provide any necessary exposure notifications in the instance that someone Jean interacted with that day tested positive shortly after the interaction.

Having this information would make the decision to grant Jean entry upon return much simpler and with increased confidence.

Exposure notification for visitors

FIGURE 3

Scenario: Alerting business contacts of test result



Monday
Jean, a contractor, visits your office

Policy
What criteria will YourCo use to grant a visitor permission to enter? Will Jean be tracked around YourCo's facility?

Data and Technology
How will data be collected? How will its integrity be ensured? How will it be stored? Who will have access to the data?

Tuesday
Jean returns to her office

Policy
What information should be used to grant Jean access to her office? How is that complemented by YourCo's information?

Data and Technology
Can JeansCo query YourCos data? How is YourCo's data shared with and verified with JeansCos system?

Wednesday
Jean tests positive for COVID-19

Policy
What information is shared back with YourCo? How does YourCo contact their employees that interacted with Jean?

Data and Technology
How is the connection maintained between JeansCo and YourCo? How is information securely shared while maintaining privacy?

Source: Adapted from data provided by Boston Consulting Group

Suppose that, shortly after visiting your office, Jean tests positive for COVID-19. If your company and Jean's company are using interoperable return-to-work applications, it may be possible for Jean's system to alert your system of possible exposure in a way that preserves everyone's privacy.

Further, there may be recorded Bluetooth handshakes with individuals with whom Jean came in close contact, providing your company with actionable data to notify specific employees of potential exposure. Absent an interoperable, secure solution, it may not be possible or legal for Jean's company to disclose her status to your company. Further, you may not have been able to track who Jean came into contact with while at your office so would not know with whom Jean was in close contact even if you were contacted.

These three scenarios illustrate the potential – and also hint at the complexity – of interoperable return-to-work applications. But the complexities are not just technical. There is a raft of ethical and regulatory issues related to data privacy, user consent and security that are perhaps even more challenging than the technology hurdles.

It should also be noted that the return-to-work challenge is closely analogous to the opportunities and challenges that exist with international travel. Rather than employers, governments need to manage entry at their borders. And there are opportunities to learn from these efforts. For instance, the European Union is developing an interoperability standard between countries called the eHealth Network "Toolbox" to allow for the safe exchange of information.

But in some ways, the private-sector challenge is more acute. Individuals who are not employees regularly interact with employees of a given company, at a frequency much greater than travel across sovereign borders or within borders.

The balance of this paper will provide an overview of return-to-work solutions available today, discuss some of the technical options to bridge the interoperability gap, propose a set of baseline ethical principles to ensure policy compatibility and, finally, conclude with a call to action for various stakeholder communities involved in the safe return-to-work discussion.

2 The current response

Key takeaways:

- Public and private solutions are rapidly emerging and evolving.
- The number and complexity of solutions is likely to grow, inducing further proliferation of standards across them.

While many governments have developed national or regional technology solutions to help limit the spread of COVID-19, they largely focus on tracing coronavirus exposure retroactively. With a few noteworthy exceptions, as with the Health Code app in China, government solutions do not even attempt to address permissions to enter some protected venues. The Health Code app works through integration with the heavily adopted Alipay and WeChat applications. Users enter symptoms that they may be experiencing and the names of individuals with whom they have come into contact. They are then given a red, yellow or green QR code indicating whether they are allowed to enter. This type of coordinated response is limited, however.

The lack of a comprehensive public solution in many countries and the need for a more specific set of features has led private employers to seek their own technology tools to help them address challenges of safely returning employees to the workplace. This has resulted in a proliferation of privately built and repurposed technologies from start-ups and multinational companies across the globe.

Despite a generally common goal, every solution is different. Each incorporates a slightly different combination of re-entry frameworks, data and features. Most solutions collect health data to initially determine if an individual is infected or at risk of being infected. This data may range from self-attestation surveys, to in-person temperature checks, to certified test results.

Many solutions, although not all, offer Bluetooth or GPS capabilities to track and trace exposure to at-risk individuals. Some (although notably fewer) offer exposure notifications to alert employees if they have been in contact with someone who is at-risk of or confirmed with COVID-19. Finally, if a user becomes sick, some solutions offer a variety of support tools, such as instructions for action or assistance in scheduling a test to confirm a diagnosis.

These solutions have already been adopted by businesses across industries. The speed at which return-to-work technology solutions have been developed and deployed speaks to the innovation in the technology space, and conversations with leaders reinforce the need for the solutions. Both public and private bodies are creating versions of return-to-work applications.

Figure 4 illustrates some of the diversity of solutions available. Since the industry is evolving rapidly, the specific capabilities of each platform may well change by publication. But the broader point is the number of solutions and the diversity of their capabilities.

Importantly, each of these solutions is a “data island” today. They work for the populations that use them, but don’t operate between them.

FIGURE 4 | Tools to help employers safely reopen

		Large Tech Solutions						Security Tech Solutions			Healthcare Solutions		
		IBM	Microsoft UnitedHealth Group	PEGA	salesforce	servicenow	Infosys	CLEAR	kokomo24/7	POP entry +	Castlight	Net Health	SafetyTek
		Return to Workplace Advisor	ProtectWell	Emp. safety & Business continuity	Work.com	Safe Workplace	Return to Workplace	Health Pass	Covid-19 Tracker	PopEntry+	Working Well	Employee Health for COVID-19	SafetyTek
Platform	Desktop	›	⊘	›	›	›	›	⊘	›	⊘	›	›	›
	Mobile	›	›	›	›	›	›	›	›	⊘	›	›	›
Health Data	Attestation	›	›	›	›	›	›	›	›	⊘	›	›	›
	Temperature	⊘	⊘	⊘	⊘	›	›	›	⊘	›	⊘	⊘	⊘
	Lab Report	⊘	›	⊘	⊘	⊘	⊘	›	⊘	⊘	›	⊘	⊘
Track & Trace	GPS	⊘	⊘	⊘	⊘	⊘	›	⊘	›	⊘	⊘	›	⊘
	Manual	⊘	⊘	⊘	›	⊘	⊘	⊘	›	⊘	⊘	›	⊘
Use Case	Social Dist.	⊘	›	›	›	›	›	⊘	⊘	⊘	⊘	›	⊘
	Dashboard	›	›	›	›	›	›	⊘	›	⊘	›	›	›
	Communicate	›	›	›	›	›	›	⊘	›	⊘	›	›	›
	Education	›	›	⊘	›	⊘	›	⊘	⊘	⊘	⊘	⊘	⊘

Note: Information is representative and not exhaustive. Reflects publicly available data as of August 2020.

Source: Adapted from data provided by Boston Consulting Group

3 The role of technology in future responses

Key takeaways:

- Relatively robust technical solutions exist for the exchanging of data.
- The key technological challenges are centred around the rules and norms of data-sharing such that the data, and individuals, are protected.
- Technical solutions can adopt one of the two approaches to securely solve the interoperability challenge. First, as seen in eHealth records, an open data approach can be leveraged and complemented with emerging privacy enhancing technologies such as homomorphic encryption. Second, data can be secured and linked via federated distributed data legers, which also requires the use of emerging technologies.
- The challenge lies in establishing a set of norms for implementing the technologies that each solution provider can follow as they rush to market.

The technical challenges of interoperability are not driven by a lack of technical ability but, instead, by the rules and norms about how data can or should be shared. Two precedents provide thought-provoking, but imperfect, analogies.

First, take air travel. Today, airlines share their passenger manifest information with security agencies so that travellers can pass through security to their gates. That data is often augmented with information about the passenger to speed their access based on a risk assessment. In the US, for instance, TSA PreCheck is a programme that pre-qualifies travellers after gathering background data on the individual. Further, flight manifests are electronically provided to immigration authorities for international flights, so that authorities are aware of who is arriving before they land. The example of air travel shows how access permissions can be granted using data shared electronically through interoperable systems across borders and entities.

Second, the healthcare industry provides a different example. Identifiable, raw healthcare data is extremely sensitive and requires exceptional caution. Electronic health records (EHRs) have, in part, standardized data collection procedures of a patient's complete medical history and allow secure access to the information to aid the decision-making of healthcare professionals in parts of the US and Europe. Yet, despite the effort, two-thirds of hospitals still send and receive at least some of their records through fax or mail.[1] This example illustrates the ability to protect and exchange sensitive data across a relatively concentrated and homogenous set of entities.

While these examples illustrate the potential benefits and challenges associated with making information systems interoperable, the healthcare case is particularly instructive for the return-to-work scenario. While EHRs share data through advanced platforms based on open data standards (HL7/FHIR in the US), this technology has not solved the challenge of sharing healthcare data. A similar technology could be used for return to work, and we could face similar challenges. Yet options exist to mitigate them.

To enable entry permissions, one option is to simply share far less data. Rather than share underlying health data, apps could simply share conclusions about safety. For instance, China's three-colour system requires users to show only whether their status on the phone app is red (high-risk), yellow (medium-risk) or green (low-risk).[2] Key, however, is to develop a consensus on some safety scale.

Another option would be for data to not be transferred at all, but to be provided by a trusted third party, such as a government or private laboratory. In this case, a visitor to a company would not need their employer's app to transfer data, but could simply provide an anonymized identifier, such as a QR code, which could be scanned by a receptionist to verify, for instance, that a negative test was conducted within a required time window.

To enable proximity detection and exposure notification however, more complex privacy-enhancing technologies may need to be used. The key to these functions is to capture a history of an individual's interactions to be able to interrogate in the future, in the event of a positive test. On a business' premises this can be accomplished by automatically logging Bluetooth handshakes when users come within a certain proximity of each other, incorporating geolocation and proximity data from wearables and smartphones, or more manual methods such as meeting attendance and location logs.

In mid-2020, Google and Apple developed a mobile-based solution for Android and iOS that enables proximity detection and exposure notification in an anonymized way that is also decentralized. The data about interactions is stored only on the phone, and the user has discretion about whether to share a positive test result, which triggers anonymized notifications to those they were recently near. It should be noted however that this solution is only being made available to sovereign governments, not private-sector customers; and, in any event, it may not meet all of an employer's needs.

This leaves two principal approaches to enabling the exchange of such data while preserving privacy. Both combine a core enabling technology with the kinds of privacy-enhancing technologies described in a recently published World Economic Forum briefing paper, A New Paradigm for Business of Data.

Option 1: Sharing data via open data centralization

Open data definitions derive their genesis from how Open XML-based technologies evolved, in which every data capture and associated unique identifier embeds its definition and structure in any message exchanged with other solutions.

These solutions traditionally lacked embedded privacy-enabling provisions to ensure encryption could not be broken and data could be manipulated in encrypted states. Emerging micro technologies can help bridge these gaps. For example, homomorphic encryption technologies can ensure that any encrypted data shared can be computed safely while encoded. Further, by incorporating fusion design principles, solutions could introduce differential privacy provisions through introduced noise in the infection data in addition to homomorphic encryption.

The simplicity of this architecture makes it very attractive, but there are several challenges in aligning stakeholders on a common architecture and standard.

Approaches like this are generally easier to pursue if the solution providers were organized through an industry or public group to align on defining these open and common standards, and there is progress being made in the COVID-19 application space with some early efforts towards establishing these organized groups. This is evidenced both in private industries with Apple and Google, for example, as well as in public entities such as the eHealth Network "Toolbox" that is being developed in the European Union

Option 2: Securing and linking data via the federation of distributed data ledgers and private sovereign data

A multitude of solutions are emerging for securing data using linked distributed and sovereign solutions. These solutions broadly leverage a combination of distributed data and private sovereign data technologies.

Distributed ledger data-based solutions can be implemented for securely linking unique identities associated with both participating trace members and infection instances along with trace inferences. Interoperability of identities is achieved as these distributed ledgers are inherently built on a standard block definition followed by all participating parties. This distributed network can be federated with sovereign private data stores that own and manage detailed data, like the location-based contact ping data generated by Bluetooth handshakes that each member generates.

Such a federated solution could leverage privacy and distributed micro technologies such as trusted execution environments (TEE), multi-party computation (MPC) and perhaps also decentralized learning, as we explore further below.

Once the infection trigger identifies the infecting globally unique identifier (GUID), the actual mapping against locally stored contact encounter data could use a distributed algorithm to do final matching. The tracing and matching is facilitated by simulations using MPC to execute algorithms in distributed fashion with decentralized learning technologies.

The US Food and Drug Administration has been engaging with health technology providers to use such federated technologies to manage COVID-19 data across clinical trials and treatment investigations.[3] A real-world illustration of this is a solution made by HealthVerity, which uses a blockchain-based self-sovereign distributed data architecture to aggregate anonymized data to facilitate interoperability between data sources.[4]

To adopt and quickly scale up an end-to-end federated blockchain network requires focus and collaboration between many stakeholders. Due to the demanding collaboration, such a solution may not be practical for our current pandemic as much as a potential solution for the next one.

Ultimately, the technology challenges are addressable. The technologies exist or are within modern capabilities and have been implemented in similar circumstances. But companies and organizations need to collaborate to agree on standards and norms. That might be hard work, but it's possible. While the technology hurdles are addressable, new blockages may emerge in differences between organizations in norms for *collecting* and *using* data. These are matters of ethical principles, or policy, rather than technology – the topic of the next section.

4 Design principles for effective development

Key takeaways:

- Even if technical qualification differences and incompatibilities can be overcome, there are still issues of data privacy, security and user consent.
- Governments and employers are learning at pace and in parallel to design their solutions to balance effectiveness with respect for individual rights.
- Like the risk of technical incompatibilities, there is a risk that policy differences might lead to their own form of incompatibility that prevents interoperability.
- To help organizations climb the learning curve faster, and in the hopes of driving some alignment to avoid this inconsistency, we have distilled eight design principles from those espoused by a range of employers and stakeholders.

While modern technology can address many of the technical challenges, the more complex challenges sit within the diversities of policies and operating norms that exist across entities. Without alignment on data policies, technical solutions to interoperability won't achieve any benefit.

Visitors to a business are not employees, and the "contract" between a visitor and a company is not the same. As such, app interoperability presents unique challenges with regard to privacy and consent.

Establishing core design principles can help create a global system of interoperable return-to-work solutions by reducing differences in data treatment. We reviewed published design principles from leading entities around the world, including governments such as the EU Interoperability Principles and the US GDPR, private corporations such as Salesforce and Microsoft, NGOs and academic institutions such as the Massachusetts Institute of Technology (MIT). The list below is a distillation of the frequent and powerful design principles being leveraged and promoted by these institutions.

1. **Company accountability**
   Take responsibility for decisions and subsequent consequences. Hire third-party auditors to validate adherence to stated policies. Allow individuals access to all their personal data in a timely manner.

2. **Data accuracy**
   Ensure data is up to date and encourage users to review data and correct inaccurate information.

3. **Data minimization**
   Collect the minimal data required to assess the health of individuals and delete data once it is no longer needed or no longer serves its intended purpose.

4. **Data security**
   During the process of data collection, storage and exchange, take necessary steps to prevent and prohibit breaches and re-identification.

5. **Explicit consent**
   Gather revocable explicit consent for data collection, processing and sharing from all individuals after they fully understand the implications of their decision.

6. **Full transparency**
   Design the technology around open-source code and data exchange protocols to facilitate auditing and interoperability. Express policies in concise, clear, plain language consumable by all individuals.

7. **Purpose limitation**
   Clearly and narrowly define the purpose of data collection around public health to prevent misconstruction and misuse. The data should be used only for the purpose agreed between the user and the collector.

8. **Legal compliance**
   Comply with and surpass legal requirements for data protection and cooperate with public bodies to develop the technologies.

Placing these eight principles at the core of decision-making, and making them transparent to users, can improve the likelihood that solutions are accepted and successful. Adoption of these principles across the parties supporting an interoperability solution can remove a set of potential policy blockers to agreement.

Conclusion: A call to action

Now is the time for employers, app developers, public officials and standards bodies to contribute to a collective solution.

Technical norms must be established to facilitate and drive interoperability. Proactively working to establish norms is a more efficient means of achieving this than retrofitting solutions. This will become more difficult over time as solutions proliferate; therefore, action is needed now.

Each stakeholder has their own contributions to make regarding technical and design principle norms. A few illustrative questions each should ask include:

Employers

- What criteria will you set for permitting a visitor on your premises?
- What criteria will be used to decide if an employee – perhaps one who has also been paying visits to customers – can return to a work location?
- How will you inform employees about the principles for data collection and usage?
- How will you interpret and navigate relevant worker protection and safety rules and regulations during this process?

Developers

- What interoperability standards can you adopt? How can you help shape these standards?
- How are you ensuring compliance with regulations as well as transparency on important design decisions that impact the design principles above?
- How can you design your products with these principles in mind to inspire confidence and, ultimately, usage?

Public officials

- What can you do to bring stakeholders together?
- What financial or organizational resources can you provide to spur innovation?
- What foreign nations can you work with to build an multinational solution?

Standards bodies

- What existing standards can be adapted to support COVID app interoperability?
- What resources do you need to establish standards rapidly?
- What other stakeholders can facilitate the creation of standards?

Resolving these challenges organically will take far too long. For the greatest impact, we need to act swiftly. Adhering to the principles individually will make a difference. Joining existing alliances, designing or leveraging common technological interoperability frameworks will have even more impact.

While COVID-19 will hopefully be with us for only a short period, efforts in the short term will aid in our collective preparedness for the next pandemic.

Contributors

Lead authors

Derek Kennedy
Managing Director and Senior Partner, Global Tech Sector Leader, The Boston Consulting Group

Stephen Robnett
Managing Director and Partner, The Boston Consulting Group

Brandon Magsamen
Principal, The Boston Consulting Group

Eric White
Head of Information Technology Industry, World Economic Forum

Grigory Shutko
Platform Curator, Information Technology Industry, World Economic Forum

Contributors

Dharmesh Syal
Managing Director and Partner and Chief Technology Officer, BCG Digital Ventures

Matt Baker
Senior Vice-President, Dell EMC Strategy and Planning, Dell Technologies

Ned Bicks
Chief Strategy Officer, Iron Mountain Information Management

Prasad Joshi
Senior Vice-President, Emerging Technology Solutions, Infosys

Peter Doolan
Executive Vice-President, Digital Transformation and Innovation, Salesforce

Jeff Taylor
Senior Vice-President, Strategy and Go-to-Market Operations, Pegasystems

We would also like to express our gratitude to World Economic Forum colleagues from four different platforms who reviewed the paper and provided valuable comments and suggestions: Genya Dana, Cameron Fox, Derek O'Halloran, Martina Szabo and Geoff Wylde.

Last but not least, it is important to acknowledge the role the Forum Information Technology Strategy Officers and CEO Deputies Community played in bringing the whole idea of the safe return-to-work interoperability research to bear, highlighting the importance of the issue and helping frame the effort.

Members of the Information and Communications Technology Strategy Officers and CEO Deputies Community

Suruchi Ahuja
Chief Strategy Officer, Tillman Global Holdings

Mikael Bäck
Corporate Officer and Vice-President, Telefonaktiebolaget LM Ericsson

Matt Baker
Senior Vice-President, Dell EMC Strategy and Planning, Dell Technologies

Andre Bechtold
Senior Vice-President, Head of Strategic and Corporate Services, SAP

Brad Berry
Chief Strategy Officer, Cognizant Technology Solutions

Ajay Bhaskar
Vice-President; Global Head, Corporate Strategy and Intellectual Property, Wipro

Ned Bicks
Chief Strategy Officer, Iron Mountain Information Management

Anand Birje
Corporate Vice-President; Global Head, Digital and Analytics, HCL Technologies

Chen Ximin
Senior Vice-President and Chief Operating Officer, Neusoft Corporation

Edmund DiSanto
Executive Vice-President, Chief Administrative Officer and General Counsel, American Tower Corporation

Peter Doolan
Executive Vice-President, Digital Transformation and Innovation, Salesforce

Dan Hushon
Senior Vice-President; Chief Technology Officer, DXC Technology

Neha Idnani
Vice-President, Head of Programs, Chairman's Office, Bharti Enterprises

Carlos M. Jarque
Executive Director, International Affairs, Government Relations and Corporate Affairs, América Movil

Manuel Kohnstamm
Senior Vice-President and Chief Corporate Affairs Officer, Liberty Global

Dimitris Lioulias
Vice-President, Corporate Strategy, Saudi Telecom Company Group

Peter Maier
President, Industries, SAP

Alexander Mathieu
Vice-President, Corporate Strategy and New Business Development, Nokia Corporation

Jagdish Mitra
Chief Strategy and Marketing Officer, Tech Mahindra

Santosh Mohanty
Vice-President, Tata Consultancy Services

Deepak Padaki
Executive Vice-President; Group Head, Strategy and Chief Risk Officer, Infosys

Matthew A. Quinn
Chief Operating Officer, TIBCO Software

Rima Qureshi
Executive Vice-President and Chief Strategy Officer, Verizon Communications

Tom Riege
Senior Vice-President, Office of the Chief Executive Officer, Telenor Group

Quincy Ross
Senior Vice-President, Corporate Development, Uptake Technologies

James Ryan
Senior Vice-President and Chief Strategy Officer, Liberty Global

Savi Soin
Senior Vice-President, Strategy and Business Development, Qualcomm

Wouter Stammeijer
Head, Corporate Strategy and Investor Relations, Royal KPN

Jeff Taylor
Senior Vice-President, Strategy and Go-to-Market Operations, Pegasystems

Marc Vancoppenolle
Global Head, Government Relations, Nokia Corporation

Florence Verzelen
Executive Vice-President, Industry Solutions, Field Marketing, Global Affairs, Dassault Systèmes

Javier Villamizar
Partner, Softbank Investment Advisers (UK)

Xuemin Wang
Director, Europe Standardization and Industry Development Department, Huawei Technologies

Jason Zajac
Chief Strategy Officer, Arm

Endnotes

1. Wise, J. (2018, December 2020). *Healthcare Business and Technology*. Retrieved from "Electronic health data transfer: Where hospitals stand right now": https://www.healthcarebusinesstech.com/electronic-health-data/

2. Ankel, S. (2020, April 7). *Business Insider*. Retrieved from "As China lifts its coronavirus lockdowns, authorities are using a color-coded health system to dictate where citizens can go. Here's how it works.": https://www.businessinsider.com/coronavirus-china-health-software-color-coded-how-it-works-2020-4

3. *PR Newswire*. (2020, 9 June). "HealthVerity announced research collaboration with FDA to suport COVID-19 clinical study and treatment opportunities": https://www.prnewswire.com/news-releases/healthverity-announces-research-collaboration-with-fda-to-support-covid-19-clinical-study-and-treatment-opportunities-301072414.html

4. *HealthVerity*. (2020, 1 July). Retrieved from https://healthverity.com/solutions/healthverity-census/

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org