MARSH & McLENNAN ADVANTAGE

DIGITAL HEALTH SURVEILLANCE

A balancing act for businesses

Kavitha Hariharan
Ben Hoster
Jaclyn Yeo

MARSH GUY CARPENTER MERCER OLIVER WYMAN

INTRODUCTION

Digital tools to monitor employee health can facilitate a safe return to work — if businesses mitigate technology and trust risks.

While COVID-19 remains a threat worldwide, societies and businesses are keen to restart economies and return to work safely[1] without causing a resurgence of infection. Some governments are rolling out digital tools in attempts to control the spread of the disease. These efforts vary across countries and regions in effectiveness, and some businesses may find it desirable to pursue their own solutions to return to work safely and sustainably before their financials and market positioning weaken further. Leading firms are already evaluating and deploying tools to track employees' health, with a view toward boosting their safety and confidence in returning to workplaces and mitigating the risk of start-stop operations.

The opportunities are multiplying rapidly. Smartphones and wearable devices can assess employee exposure and transmission risk, facilitate contact tracing, and rapidly isolate new cases and close contacts. Augmented-reality tools can help employees maintain safe distancing in high-traffic sites, such as manufacturing shop floors and distribution warehouses. Mobile apps can be used to push critical alerts, provide facility status updates, and monitor employee sentiment.

While employers have long used monitoring technology — for example, keystroke tracking, screen grabs, website visits, and geolocation delivery route monitoring to measure employee productivity — health surveillance can seem an Orwellian overreach. Businesses need to determine what, if anything, might be appropriate and viable in the context of their communities, circumstances, and culture. This paper looks at the currently available options: their benefits, risks, trade-offs, and implications for a sustainable implementation.

In reigniting economic activity, businesses — and governments and societies — need to balance the imperatives of public health and individual liberties, and to do so against a backdrop of widespread concerns about personal data exploitation, the slippery slope of surveillance, and potential cyber incursion. Employers that get the balance right will not only strengthen their results and competitiveness but also reduce liability exposures and foster enduring employee trust and loyalty.

1 Oliver Wyman (2020). The Great Balancing Act. Retrieved on 29th May 2020, from https://www.oliverwyman.com/our-expertise/insights/2020/may/the-covid-19-oliver-wyman-pandemic-navigator-insight-number-two.html

Digital Contact Tracing And More

While digital tools by themselves are unlikely to control the spread of COVID-19, they could complement existing public health interventions to further mitigate the severity of outbreaks. (See Exhibit 1.) Similar digital solutions could also help prepare businesses for a safe return to the workplace.

Exhibit 1: Identifying emerging technologies and opportunities to address business challenges

Opportunities	1. DIGITAL CONTACT TRACING	2. WELLBEING AND SENTIMENT MONITORING	3. REPORTING AND ANALYTICS
	Digital proximity-tracking applications use the closeness of mobile phones as an indicator or contact between people, recording multiple interactions that may be forgotten by those testing positive	Employees experience varying levels of stress based on their working environments and personal circumstances. Understanding their needs and providing targeted support can improve workforce wellbeing and productivity	As with any aspect of the business, the ability to report key measures and respond appropriately to negative developments is essential for maintaining workplace safety
Potential features	• Identifying individuals who might have come into contact with a positive case • Alerting identified contacts • Providing instructions on next steps — for example, testing or quarantine	• Wellbeing pulse checks • Micro surveys/chatbots	• Outbreak intensity monitoring (global, regional, company) • Workplace safety metrics • Local facility operability metrics
Value for business	• Identify and break chains of transmission • Guide workplace responses: direct disinfection efforts, prescribe enhanced PPE use	• Increase employee engagement • Strengthen support for physical and mental health needs of staff	• Improve facility status updates and employee awareness • Inform decision-making by pandemic response team
Relevance	• Workforce • Customers or visitors to the workplace	• Workforce	• Workforce • Board of directors • External parties — for example, insurers or investors

Source: Oliver Wyman, Marsh & McLennan Advantage

DESIGN CHOICES

No single tool will suit all. To develop digital health surveillance that is appropriate and fit-for-purpose, businesses must first understand what technology can and cannot do: the operational principles, available options, and pros and cons.

Businesses should begin by weighing what they need to accomplish versus what would be nice to have. For example, a primary purpose might be preventing clusters from forming at the workplace, to minimize further disruption to business operation. Other potential objectives include avoiding infecting customers, managing employee health, providing support services. Depending on its needs and priorities, each business can evaluate foundational choices with respect to data to be collected, coverage of the tool, and data management.

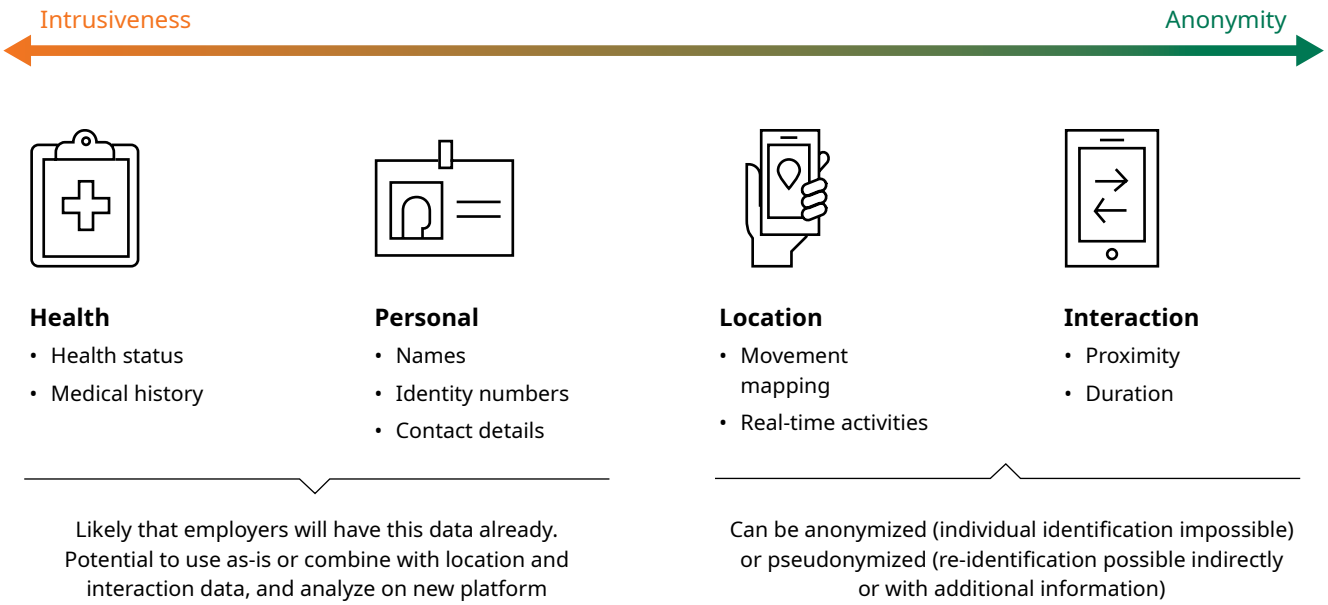
WHAT DATA TO COLLECT

Confinement to a core objective and collection minimization should serve as the guiding and driving principles for collecting data. Rather than casting a wide net to capture what might prove useful, collect only what is absolutely necessary to achieve the set objective, and set limits up front on how long the data will be stored and used.

Consider the objective of preventing a "lockdown" of a worksite, by facilitating targeted and timely isolation or quarantine of employees at risk of transmitting the virus. The minimum data required to identify and notify close contacts of cases are indicators of distance and duration of contact. This can be done by anonymous, dynamic identifiers generated by a proximity-tracking app, which can also carry out an automated risk assessment, notify the device owner, and advise on next steps. This use case does not necessarily require personal, health, or location data — unlike alternative scenarios in which employers want to do more to manage employees' health, such as monitoring symptoms or movements to facilitate testing and treatment.

Broader data sets expand an employer's ability to implement more comprehensive response measures, but the drawbacks should not be neglected. (See Exhibit 2 on the next page.) Taken in concert with hastily deployed technologies that may pose new risks, they present an attractive target for cyberattacks and fuel employee fears of data exploitation and creep beyond the original scope and objectives. Besides considering and addressing privacy and security challenges, businesses should also communicate the precautions clearly, so that employees feel comfortable with sharing the necessary data.

Exhibit 2: Different digital health surveillance purposes for different data requirements



Source: Marsh & McLennan Advantage

FROM WHOM AND HOW

Business needs and situation should guide decisions on who should be covered by a digital surveillance tool: some or all among the employees stationed at a site, employees visiting from other sites, visitors and customers? Another question for businesses is whether to limit monitoring to the worksite and work hours, or to extend it to other times and places such as commutes and work travel.

Every business will need to comply with regulations, which differ across jurisdictions with respect to whether employers are required, allowed, or forbidden to collect health-related data from employees stationed at worksites or non-employees. For example, businesses in Singapore are required to collect personal data and contact details of any individual entering their premises and to share the data with public health authorities for contact-tracing purposes. Other countries, such as the United States, may offer varied or limited guidance, leaving more room for employers to evaluate options. However, this may inevitably increase liability risks for employers and hence discouraging them to adopt these digital solutions.

Inclusion and efficacy are two other considerations for businesses. Tools should be designed so they do not exclude employee segments with limited digital literacy or device access. For example, issuing a separate wearable device may be a potential solution for lower-wage workers who are less likely to have their own devices and more likely to work on site. More comprehensive data sets — such as those that cover everyone, beyond worksites and hours — will expand the analytical capabilities of a digital surveillance tool and could increase its accuracy. Mass surveillance, however, will not be feasible or acceptable in some jurisdictions, industries, or organizational cultures, and, even when possible, may spook employees and risk a backlash.

Businesses must also decide whether to mandate or persuade users to adopt the tool. (See Exhibit 3.) Mandated or coerced use — for example, making utilization of the tool necessary for continued employment or access to basic services — is recommended only if the tool is essential for compliance with local regulations. Voluntary implementation, however, will reduce the tool's uptake and effectiveness, particularly if employees lack confidence in its utility and protections. At the same time, voluntary implementation lowers reputational and liability risks, making challenges less likely from employees, unions, or external organizations such as civil liberties groups.

Exhibit 3: Implementation approach will affect uptake and trust

Mandatory

Utilization compelled by policy or legal requirements

Coerced

Utilization made necessary to access services requirements

Voluntary

Utilization based on free choice and willingness to use

Source: Marsh & McLennan Advantage

WHERE TO STORE AND PROCESS DATA

When deciding between two dominant models for data storage and processing, businesses should consider the trade-offs between control, capabilities, and trust, as well as the risks associated with each option. (See Exhibit 4.)

A centralized model puts a designated server — together with the support team at the business — in a position of trust and authority, with the power to aggregate and analyze the data collected. Taking digital contact tracing as a use case, a centralized approach increases the visibility of the issue for a business and enables it to take charge of executing key actions: for example, mapping social interactions, identifying specific employees at risk of exposure and transmission, notifying and advising on next steps, and supporting and monitoring compliance. At the same time, vast data sets could present an attractive target for cyberattacks and elevate the prospect of mission creep and the exploitation of the data and tool for other purposes in the future.

Exhibit 4: Centralized versus decentralized models

Centralized

- Data gathered and uploaded to remote server
- One or more entities (for example, health authority, company) have access to whole data set

VS.

Decentralized

- Data stored and processed locally on individuals' own devices
- No single entity has access to whole data set

Source: Marsh & McLennan Advantage

Conversely, a decentralized model protects privacy by design and default, with data processing for each individual performed locally on their device. This precludes a business from achieving a full view and control over the outcomes, confers trust and authority on the tool, and relies on users to do the right thing (such as self-isolating upon receiving exposure notification alerts). At the same, a decentralized model mitigates the risk of employer abuse and the legal and reputational problems that may ensue; it also increases the likelihood of employee trust and uptake of the tool. Moreover, while many endpoint devices widen the overall attack surface, data anonymization and local storage may result in less cyber risk to the overall data set.

SUCCESS FACTORS

For successful implementation, businesses will need to offset technical limitations, earn employee trust, and comply with evolving regulations.

Even the most carefully designed digital tool for health surveillance will not be a silver bullet. To gather reliable data and deliver expected results, tools need high levels of adoption and compliance from users. That this is difficult to achieve is evidenced in government-led tools, for which uptake remains well below the necessary 60 percent of the population.[2] Technical limitations stand in the way, along with behavioral and compliance challenges.

TECHNICAL LIMITATIONS

Take digital contact tracing again as a use case. As with diagnostic tests, no digital approach to proximity tracking is perfect, and false signals may prompt harmful responses. Apps on mobile phones are likely to be blind to some transmission barriers and risk factors for COVID-19 — such as walls or poorly ventilated enclosed spaces — and may underestimate indoor exposure or overestimate outdoor exposure, depending on the risk assessment algorithm. Furthermore, the technology could be misused or abused by users (misreporting by one individual could send the whole team or office home) or malicious attacks (jamming signals), among others. Repeated false alarms would likely cause alert fatigue or result in a decline in confidence among users, which would erode compliance; false negatives might breed complacency and entice users to let their guard down and neglect proven measures such as hygiene and social distancing.

User convenience and security present another challenge. Take, for example, geolocation technologies such as Bluetooth, the most common enabler for digital proximity tracking. By default, mobile operating systems allow apps to run Bluetooth scans infrequently and for short periods of time to preserve battery life. Apps that require users to override this feature — for example by keeping their phones unlocked and the app active — expose users to inconvenience as well as security risks, such as identify theft if the phone is stolen. As many governments have learned in the past few months, device manufacturers such as Apple and Google can provide a solution, but only for government apps that meet their standards for security and privacy.[3]

2 The Wall Street Journal (2020). Apps to Track the New Coronavirus have an Old Problem: Getting the Downloads. Retrieved on 18th May 2020, from https://www.wsj.com/articles/apps-to-track-the-new-coronavirus-have-an-old-problem-getting-the-downloads-11588115728

3 Apple (2020). Apple and Google partner on COVID-19 contact tracing technology. Retrieved on 3rd July 2020, from https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

EMPLOYEE RESPONSE

Public health measures depend on public trust, and this applies also to employee health surveillance. Besides designing digital tools that balance public health and individuals' privacy, businesses should make a compelling and transparent case to their workforce for using the tools and sharing data.

Employers can frame the benefits in reciprocal terms. For example, an effective digital tool can facilitate returning to the workplace while reducing employees' risk of contracting the coronavirus or transmitting it to colleagues, family, and friends. Depending on the tool's features, employees may get exposure notifications, guidance, and support for medical interventions, alerts to avoid high-traffic choke points, hygiene and distancing reminders, and so on. Positive employee behaviors will help employers keep workplaces open, sustain jobs and incomes, and encourage stronger trust, loyalty, and performance from personnel.

If employees perceive nonreciprocal compulsion, they may disengage, push back openly, or channel their resourcefulness into finding ways to game the system — all of which will result in less reliable data and a less effective digital tool, as well as lasting damage to morale and productivity. Businesses that fail to secure buy-in from employees risk financial, operational, and reputational costs of localized virus outbreaks, office closures, workplace liabilities, and talent attrition.

CHANGING RULES AND NORMS

Digital tools for health surveillance will need to adhere to local laws and adapt to changing regulations. Multinational companies that operate in many jurisdictions will need local knowledge and agility to respond to varied and fluid situations, for reasons of compliance as well as for the effectiveness of digital tools.

To gather reliable data and deliver expected results, tools need high levels of adoption and compliance from users

This pandemic has seen some nation states prioritize public health over individual rights (for example, China and South Korea), while others are standing firmly by their commitment to data privacy and civil liberties (Austria, Canada, and Denmark, among others).[4] Laws, guidance, and expectations are changing as public debates play out with regard to government-led digital surveillance efforts. For example, as the perceived threat level of COVID-19 changes with the ebbing and flowing of waves of infection, rules on medical exams permitted by employers may change[5] — and a similar shift may apply for health surveillance also.

Gaps and uncertainties in regulations raise questions for businesses with regard to policies for, and the implementation of, digital tools. For example, what are the key criteria to set an appropriate budget to develop and deploy a tool? How might employer liability change following the implementation of the tool? Can the tool reduce the cost of the necessary insurance relating to workplace health and safety?

Even in less regulated jurisdictions, businesses should go beyond minimum standards to mitigate risks and ensure the efficacy of digital tools. Scenario modeling will help businesses make decisions and plan contingencies for a range of potential changes — to data privacy and security laws, employer liabilities, employee expectations, and so on — to build secure, compliant, and adaptable digital tools.

4 MIT Tech Review (2020). A flood of coronavirus apps are tracking us. Now it's time to keep track of them. Retrieved on 3rd Jul 2020, from https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

5 BRINK News (2020). Employment Liability Claims Set to Rise With COVID-19. Retrieved on 3rd Jul 2020, from https://www.brinknews.com/covid-19-opens-the-door-to-employment-practices-and-wage-and-hour-liability-claims/

GOOD GOVERNANCE

Governance is key to implementing any digital health surveillance successfully. To mitigate risks and ensure the system works as intended, businesses should ensure adequate safeguards, oversight, and communication.

How do businesses address technical, behavioral and compliance challenges presented by digital health surveillance? The way forward involves effective governance across the lifecycle of the digital tool. Businesses should establish and enforce safeguards, ensure effective oversight, and inform as well as consult employees to foster trust and engagement.

SAFEGUARDS AGAINST ERRORS AND ABUSE

Businesses should establish precautions across the lifecycle of the digital tools. (See Sidebar: “Sample safeguards” on the next page.) During the design and development phase create, and codify technical and policy measures to protect data privacy and security, prevent abuse, and find and fix bugs. During the deployment and maintenance phase, pursue a proper due diligence of technology partners and evaluate the tool regularly. During the decommissioning phase, audit the process, performance, and results of the implementation and report findings to leadership and the board to support preparedness for future crises.

ONGOING OVERSIGHT

Businesses should assemble an internal task force of key stakeholders independent of the project team to scrutinize implementation and enforce safeguards across all phases of the tool’s lifecycle. Convene this group from critical roles that align with business and employee needs for scrutiny — in other words, business leadership, human resources, legal counsel, and employee representatives — and ensure all members are esteemed for their integrity and competence. Also consider the value of additional oversight by objective, independent, and reputable third parties. The task force should oversee all phases of the tool’s lifecycle and be accountable for appreciating the risks, ensuring key concerns are well discussed, and validating both expected results and the implementation of corrective actions when needed.

TWO-WAY COMMUNICATION

Throughout the tool's lifecycle, senior business leaders should relay and update relevant information, such as goals, operational principles, expectations, and safeguards. Build the case for why the digital tool is necessary, what it will be used for, how it will help the business and employees, and what protections are in place against potential pitfalls. Ensure employees can access the oversight team, who should acknowledge and act on feedback. Consistently honest and transparent communication — of good news as well as setbacks, trade-offs, and uncertainties — will help build employee trust and willingness to participate in digital health surveillance.

In navigating the next phase(s) of the pandemic, it's vital that businesses protect employees' physical, mental, and financial health — and ensure high levels of engagement and productivity. Should firms choose to move ahead with digital health surveillance as a solution to return to work safely, employers would do well to remember: Employees should be monitored not with an iron fist, but with open arms.

Sample Safeguards

Technical features to preserve privacy by design and default, and to include people lacking devices or digital literacy

Strict limits on data collection, processing, and storage: minimization[1] (only necessary data), purpose (as explicitly specified), access (by whom), duration (for how long), and so on

Sunset clauses[2] to dismantle the system as well as ongoing data deletion after predetermined time frames

Data and output checks using common sense and independently verifiable results

Defenses against mission creep and misuse of data, such as provisions against the use, sale or sharing of individuals' data without their free and informed consent or beyond the tool's original purpose

Clear, transparent disclosure of data collection, processing, and storage arrangements, as well as privacy precautions for staff reassurance and compliance

Full transparency of mechanisms for feedback, whistleblowing, redressal, and penalties, in the event of any unauthorized use or misuse by internal teams or technology partners

1 Baker McKenzie (2020). COVID-19 Data Privacy & Security Survey. Retrieved on 2nd June 2020, from https://www.bakermckenzie.com/-/media/files/insight/publications/2020/04/covid19-data-privacy--security-survey17-april.pdf

2 Financial Times (2020). Data can be a powerful tool against coronavirus. Retrieved on 14th May 2020, from https://www.ft.com/content/48739142-735c-11ea-95fe-fcd274e920ca

ABOUT MARSH & MCLENNAN COMPANIES (MMC)

Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's 76,000 colleagues advise clients in over 130 countries. With annual revenue of $17 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market- leading businesses. Marsh advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and wellbeing for a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit mmc.com, follow us on LinkedIn and Twitter @mmc_global or subscribe to BRINK.

AUTHORS

Kavitha Hariharan
Director
Healthy Societies
Marsh & McLennan Advantage

Ben Hoster
Director
Transformative Technologies
Marsh & McLennan Advantage

Jaclyn Yeo
Research Manager
Insights
Marsh & McLennan Advantage

CONTRIBUTORS

Many thanks to the following individuals at Marsh & McLennan for their perspectives and inputs on this topic: Cindy Gentry, Kate Brown, James Crask, Ethan Murray, Larissa De Lima, John Rudoy, Leslie Chacko, and Richard Smith-Bingham.