Telehealth take-up: the risks and opportunities

Healthcare report 2021

kaspersky BRING ON THE FUTURE

Learn more:
kaspersky.com

Contents

Introduction

The pandemic changed the way everybody around the world interacted on a personal and professional level – this was particularly true for the healthcare industry. Most medical institutions globally were overwhelmed by patients and even after the deluge subsided, practitioners needed a way to diagnose the public without putting themselves at risk.

The solution to this has been the implementation of telehealth capabilities in which health workers talk to and sometimes even diagnose patients remotely.

Despite the global take-up of telehealth, it comes with its risks, as the extremely sensitive nature of personal data being collected, shared and stored by the healthcare sector is of **particular interest to cybercriminals**.

Healthcare professionals see a continued future with telehealth solutions, but many of them also believe that this will only be sustainable if there is a global improvement of data security for the solution.

This report will address the challenges faced by a global rollout of telehealth and how the healthcare industry can better protect the data of its patients.

Methodology

Kaspersky commissioned Arlington Research to undertake quantitative online research amongst sole or joint decision-makers working for frontline healthcare service provision (including telehealth) for new technology implementation, digital transformation or developing strategy for new technology.

389 interviews were conducted globally with representation across North America, Europe, MEA, APAC, LatAm and Russia and CIS. Survey was completed across 34 countries.

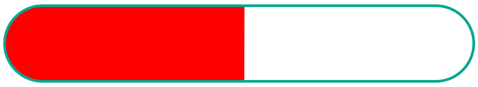
170 interviews were completed with enterprises with 1000+ employees with the remainder of interviews from organizations with 50-999 employees.

Key findings

91%
of global healthcare providers

have already implemented telehealth capabilities and the majority of them only started to use telehealth after the pandemic began

52%
of global frontline remote telehealth providers



have experienced cases where patients have refused to have a video call with medical staff due to not trusting the technology or privacy or data concerns

73%
of global frontline healthcare providers

currently use medical equipment with a legacy OS

32%
of respondents

agree their organization has faced cybersecurity issues due to vulnerabilities in third-party technologies ((33% experienced data leaks, 32% DDoS attacks, 32% ransomware attacks)

30%
of telehealth providers

agree some of their clinicians have had their patients' data compromised when conducting remote telehealth sessions

37%
of the medical community

agree that in the next 20 years technologies will be able to completely replace doctors

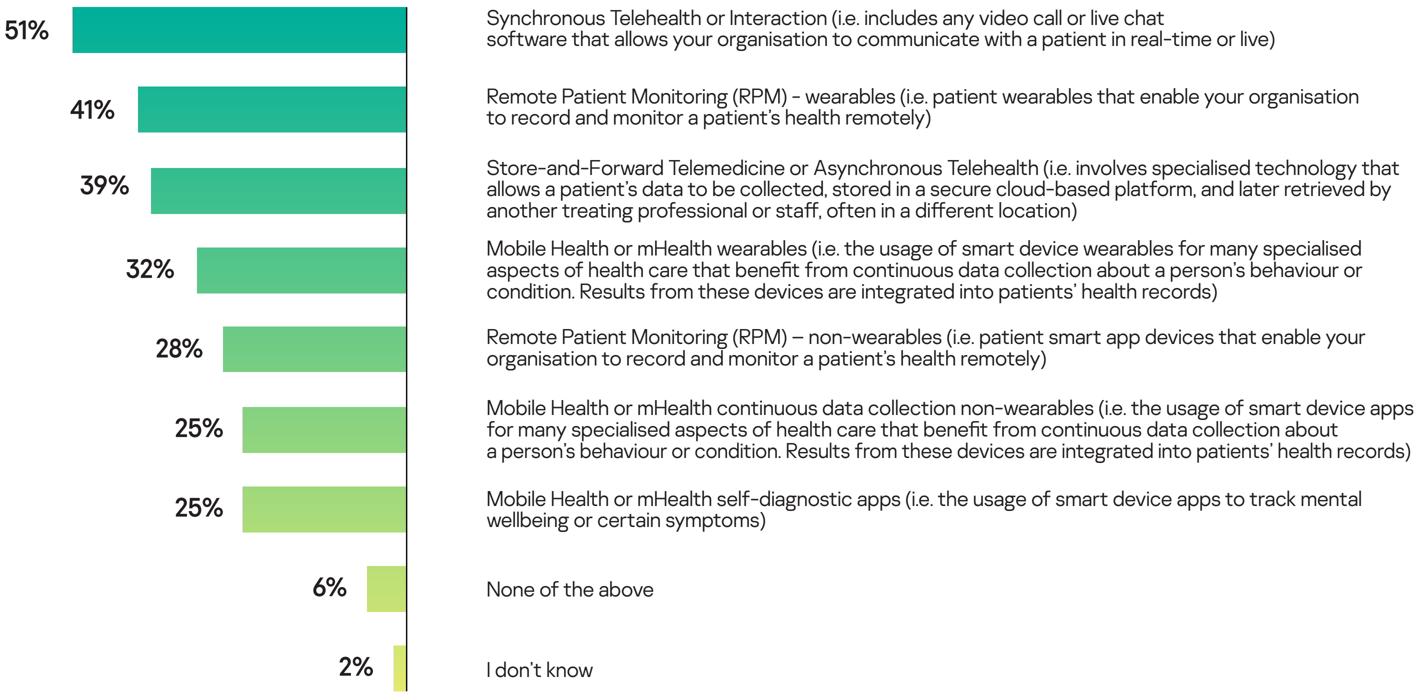
The state of telehealth

Convenient, safe, and less resource-intensive, telehealth services have been well received by the healthcare industry and the patients it cares for.

Survey data backs this up, with nine out of ten (**91%**) medical providers having already started using telehealth – providing one or more type of this service – and **44%** of global healthcare providers started using telehealth services after the pandemic started. Meanwhile, only one in five (**21%**) respondents began using telehealth capabilities less than a year before the start of the pandemic and **34%** began using these solutions more than a year before.

The most popular service in this category is synchronous telehealth or interaction, with half (**51%**) using this service, closely followed by remote patient monitoring (**41%**), and then Store-and-Forward Telemedicine or Asynchronous Telehealth (**39%**) pulling in third. In terms of general tech, when it comes to remote health checking, half of global healthcare providers leverage data from wearables.

Which of the following telehealth services does your organization provide?



Medical organizations are seeing the preference from their patients first-hand, with four in ten (**42%**) agreeing that the majority of the telehealth recipients are more interested in telehealth sessions than in-person ones due to convenience.

In terms of who is taking up the service, age doesn't seem to be a barrier, with just a half (**51%**) of healthcare providers surveyed agreeing that the majority of their organization's patients were under the age of 50.

At the extreme take-up end of the telehealth spectrum, **13%** of healthcare providers have switched completely to online consultations on a regular basis and almost a half (**46%**) are likely to do this in the future.

Concerns and challenges

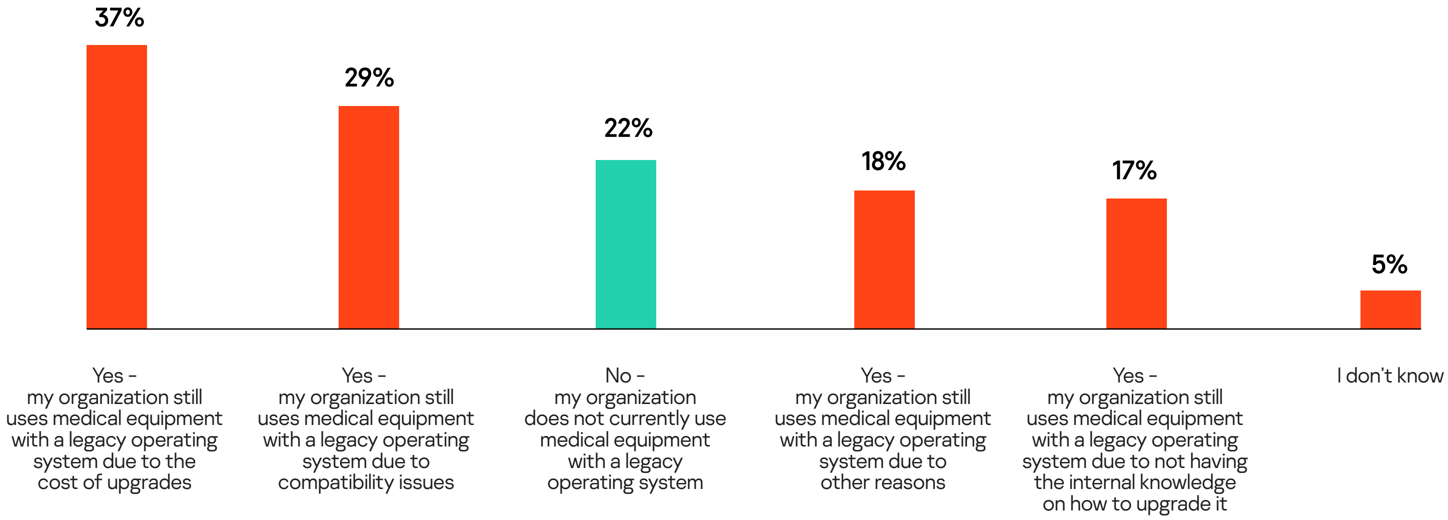
The rapid take-up of telehealth has introduced a wealth of concerns about its safety, with most patients and clinicians worried about the level of health-related data protection.

Half (**52%**) of remote telehealth providers have experienced cases where patients, not trusting the technology, have refused to have a video call with staff – citing concerns about privacy and data safety. Clinicians have also voiced their own reservations, with eight in ten (**81%**) raising concerns over conducting remote telehealth sessions. These include concerns about how patient data will be used and shared from these sessions, as well as the security of data and any personal penalties that might arise in the case of a leakage from a remote consultation.

One major challenge to the use of this emerging technology is that the technical equipment for it is far from perfect and needs improving in line with global take-up. Worryingly, three in ten (**34%**) remote telehealth providers agree that one or more clinicians in their organization have made a wrong diagnosis because of poor video or photo quality.

When it comes to the safety afforded by operating system upgrades, seven in ten (**73%**) healthcare providers currently use medical equipment with a legacy OS. Reasons for this include the cost of upgrades being too high (**37%**), compatibility issues (**29%**), not having the internal knowledge on how to upgrade (**17%**), and other reasons (**18%**).

Does your organization currently use medical equipment with a legacy operating system (OS) and if so, what are the main reasons for this?

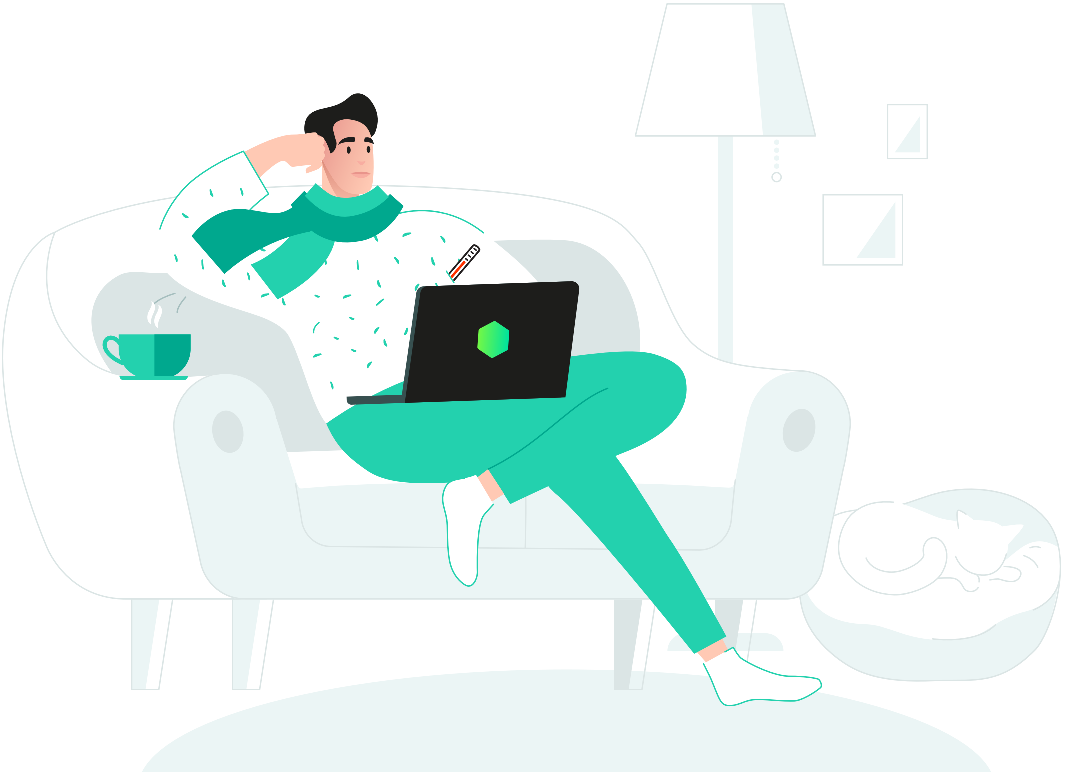


Three in ten (**29%**) also shared medical data with third parties for medical or marketing research using an email attachment without a password or digital messenger service.

Lastly, half (**54%**) of telehealth providers agree that some of their clinicians conduct remote appointments using apps that are not specifically designed for remote medical sessions with patients. These included FaceTime, Facebook Messenger, WhatsApp, and Zoom.

Many global healthcare providers have fears about the cybersecurity readiness of their organization and in most cases, they cannot guarantee data privacy and safety. Only three in ten (**30%**) respondents are very confident that their company can effectively stop all attacks/breaches of its perimeter. Slightly better was confidence in their organizations having adequate hardware and software IT security protection (**34%**), multiple back-ups for all servers, accounts, and documents (**38%**) and the necessary measures in place to safely use telehealth (**38%**).

In addition to not feeling confident about their organization's data handling, four in ten (**42%**) agree that the majority of clinicians don't have clear insights into how their patients' data is protected.



Current and future risks

Between a lack of knowledge and unpreparedness of the threat landscape, half of global respondents agreed their organization had experienced cybersecurity issues including data leaks, DDoS or ransomware attacks.

Over a third (**33%**) of respondents agree that their companies have faced these problems due to vulnerabilities in third-party technologies, with these being split between data leaks (**33%**), DDoS (**32%**), and ransomware (**32%**).

Almost a third (**30%**) also agree that some of their clinicians have had their patients' data compromised during remote health sessions.

It isn't all bad news however, as most healthcare providers are aware of how important cybersecurity is and have taken steps to mitigate the potential damage from cyberattacks. Seven in ten (**70%**) respondents agree that their organization has a dedicated IT security awareness training for all employees whose work involves technology.

Tech and healthcare: still a bright future

Despite the risks, there is still a positive future in store for telehealth and the general use of technology when it comes to health, with most of the medical community agreeing that telehealth and medical technologies will flourish and revolutionize the whole industry.

In support of this, seven in ten (**71%**) agree that telehealth services will add the most value to the healthcare sector in five years' time in comparison to any other technology.

“

Dr Peter Zeggel, CEO of the leading German telehealth provider arztkonsultation.de, shares his outlook on how telehealth technology will change healthcare.

At its core, telehealth is an enabler for a more connected approach to healthcare. Bringing patients and doctors closer together is much more than a superficial idea. Instead, the push for telehealth will initiate various significant changes to the operating principles of healthcare.

Easier access will chance perception of healthcare

Telehealth will radically increase the availability of healthcare as time and location lose much of their current relevance. Medical staff and patients can attend video consultations and use advanced medical devices from almost anywhere. Accordingly, consultations, diagnoses and treatments will be easier to attain. In addition, the point of care will move from providers into homes. This is especially important for the elderly, disabled and chronically ill or for underserved regions.

Communication is key

Increasingly specialized healthcare providers will achieve better outcomes for complex treatment cases, but they also require close collaboration. As a consequence, doctors will communicate more than ever. Teleconsultations and technology such as remote patient monitoring (RPM) will mutually complement each other in fostering closer collaboration between patients and doctors as well as between doctors.

Doctors need to adapt to changing circumstances

Like any new tool, telehealth requires training. Although doctors usually participate in continued education, only a small portion of training covers new technological capabilities. Therefore, telehealth currently advances much faster than many physicians can adapt. However, doctors will learn to trust and interpret data and utilize telehealth for close collaboration with time.

The trend towards integrated providers

Modern workplaces consist of a multitude of complex processes and applications, which need to work together seamlessly. This is especially true for healthcare. Therefore, the market will favor integrated software providers who offer versatile data interfaces and comply with established interoperability standards. However, any openness for third-party integrations comes with a cybersecurity risk.

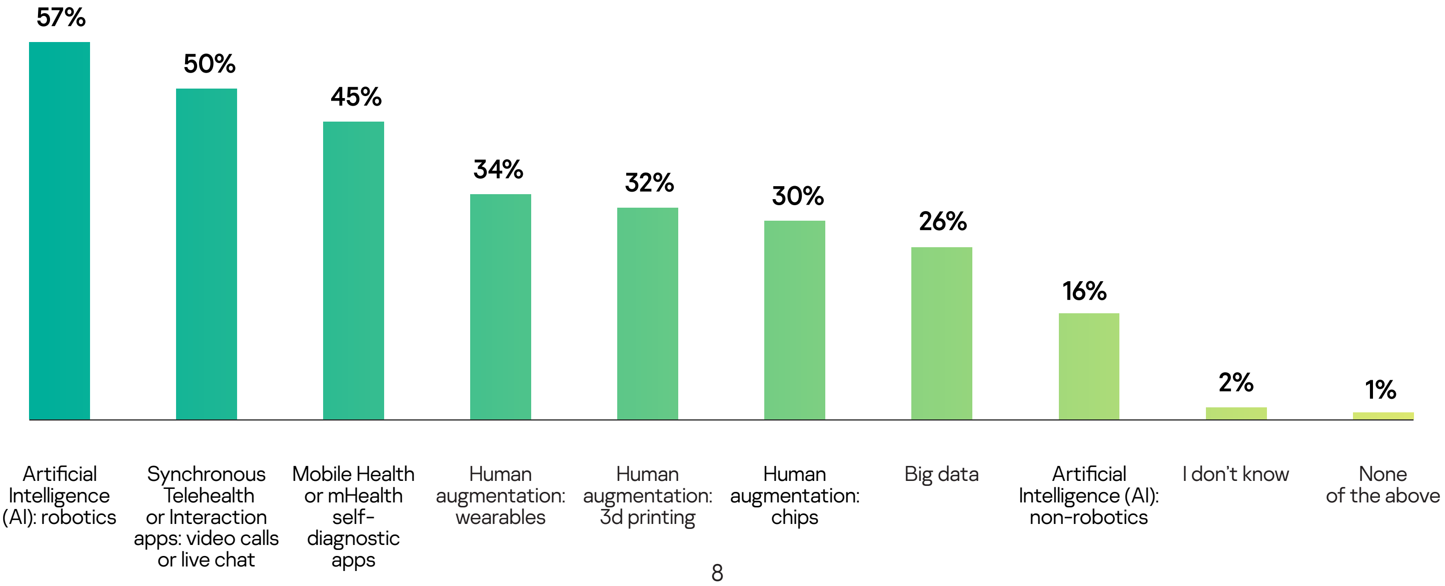
For the future, **37%** of respondents think that technologies will completely replace doctors in the next 20 years with half (**48%**) of those questioned also believing that new solutions will be so advanced that they will be able to reveal the cause and year of death.

Experts believe that data collection is one of the most important aspects for medical technology development, but they also acknowledge that there are obstacles that may prevent the gathering of required information. When it comes to this aspect of healthcare technology, almost seven in ten (**67%**) respondents agree that the industry needs to collect more data than current levels to train AI for reliable diagnostics. Six in ten (**61%**) also believe that in the future, more equipment, even personal devices will aid the effort to collect more healthcare data.

Trust in healthcare technology was something which came out strongly in the research, with almost four in ten (**38%**) respondents agreeing that they trust advice from AI more than that of colleagues, while **40%** said that in the future they would be happy to recommend their relatives to have surgery done by robots.

Despite the positive outlook, half (**48%**) of respondents believe that government and ethical restrictions will result in fragmented health-related data collection, which will worsen the accuracy of AI. Other future concerns included half (**51%**) of those asked agreeing that they would not trust AI alone when it comes to diagnosing their relatives and six in ten (**57%**) confirming that they are afraid that robot surgeons could be hacked and injure patients.

Which of the following types of healthcare technology, do you think will add the most value to the healthcare sector in five years' time?



“

Prof. Chengyi Lin, Affiliate Professor of Strategy at INSEAD and a leading expert on digital transformation

Digital health readiness: global optimism with regional variations

“Necessity is the mother of invention.” When thinking about digital health over the last few years, we may go one step further to say necessity is the mother of invention and adoption, as we all embrace technology that may not have been considered essential prior to the pandemic.

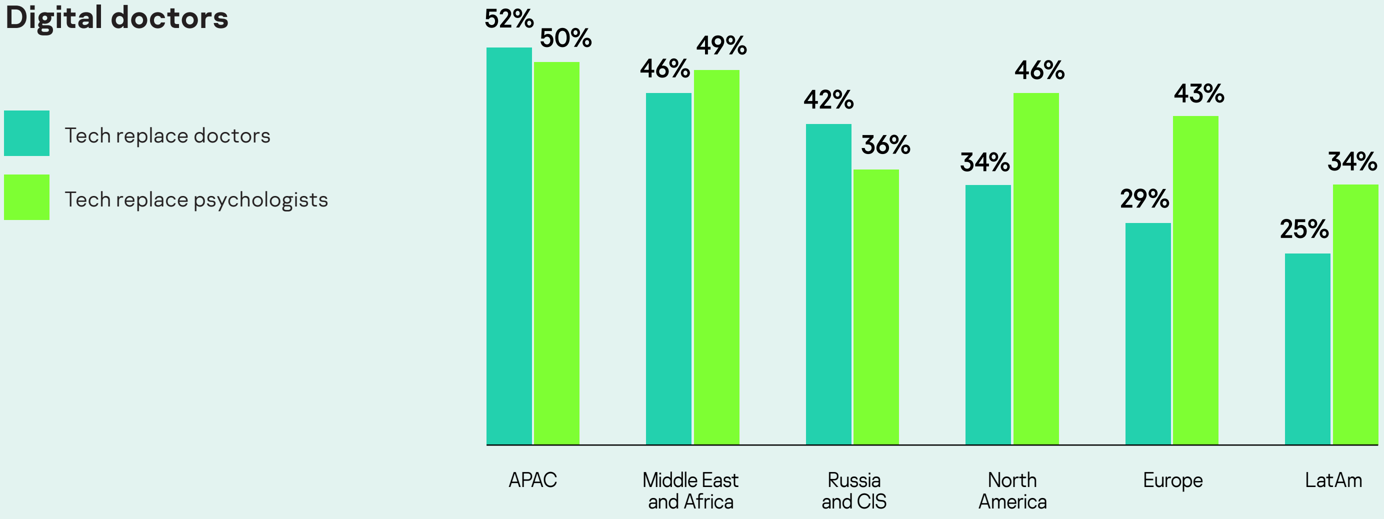
In 2020, virtual visits to receive advice and treatment for primary care and chronic health conditions in the US increased from **5%** and **6%** to **45%** and **41%**, according to a recent Deloitte survey. In the same survey, **52%** of organizations have made significant changes in their virtual health strategy in response to the pandemic. The adoption of telehealth is universal, we have seen Babylon Health offering digital services and Doctolib scheduling online consultations in Europe, AliHealth expanding AI/ML-powered services and Ping A Good Doctor strengthening its digital services through its physician platform in Asia. The significant acceleration of telehealth is primarily driven by necessity, including quarantine regulations, risks of contamination, an increased volume of consultation requests, cost pressure, and more.

Although the healthcare industry has been historically conservative and slow to adopt digital technologies, for example European pharma have been slow to adopt AI, the “COVID effect” pushed patients and healthcare providers to embrace telemedicine much quicker.

Taking a closer look, Kaspersky’s Telehealth report data suggests that healthcare providers have become more optimistic about the positive impacts of digital technologies. The increasing use of telemedicine and mobile apps continue to build confidence and reduce the perceived risks of digital health. At the same time, as the Kaspersky study has shown, the specific projections of digital health adoption vary across regions.

Asia Pacific (APAC), Middle East and Africa (MEA), and Russia are most optimistic about digital doctors. Over **52%** of healthcare professionals in APAC believe that digital technologies can replace doctors in the next 20 years, while the percentage for MEA and Russia is **46%** and **42%**, respectively. By comparison, only a third, or **34%**, in North America are as optimistic. The percentage in Europe, not surprisingly, is even lower at **29%**.

Digital doctors



The difference across regions may be partly caused by the emphasis on digital health in the public eye. For example, a series of remote surgeries were done with the help of digital technologies in China in 2019, ranging from animal operations to minimally invasive heart surgery to brain insertion surgery. These publicized advancements helped to build awareness and confidence in both the medical community and the general public.

By contrast, the projection of the replacement of psychologists by the same medical communities is more consistent across the regions at around **40%**. This may be attributed to the maturity of the relative technologies, such as text analysis, natural language processing (NLP), speech-to-text, text-to-speech, etc.

At the same time, MEA, APAC, and Latin America believe that AI and big data can drive more value for healthcare by 2045, while North America and Russia consider telemedicine and mobile health (i.e. apps) are the most valuable drivers. In comparison, the considerations of wearables stay relatively consistent across regions.

Many factors could contribute to these different views on the value of various technologies. One such example could be how the regions organize their digital innovations.

For example, digital innovation in the US tend to be specific within an industry, i.e. Uber and Lyft for ride-sharing and AirBnB for travel. On the other hand, in the Middle East and China, Supper Apps can integrate services across industries, i.e. MTDP provides multiple lines of services from airline tickets to hotel booking and food delivery to concert tickets. These supper App has demonstrated the power of AI and cross-sector data.

Another factor could be the emphasis regional governments and businesses place on AI/ML and data analytics. For example, AI Everything Summit in Dubai, which I spoke at in 2019, was positioned to be the largest AI conference in the world. The digital advancements in multiple industries and the general interest in technologies such as AI/ML may influence how healthcare professionals and patients welcome them into the healthcare industry. The co-evolution with other industries in the regional context may also affect development speed, thus reinforcing the difference of digital health evolutions across the regions.

The Healthcare sector has demonstrated its agility and solidarity throughout the COVID pandemic. The fast ramp-up of telehealth increased optimism regarding digital health. We must continue the momentum and build the readiness on technologies, patients, and providers.

Conclusion

Our research has shown that there is a strong mixture of hopes and doubts among respondents when it comes to healthcare technology. The opportunities, particularly in the new normal, where physical contact is being limited, are clear to patients and clinicians alike.

The move towards remote appointments and diagnoses was already in full swing before the pandemic, but this has gone from strength to strength as the world went in and out of lockdown. A quick switch to any type of technology on such a grand scale is always going to cause concerns but some unresolved issues related to use of telehealth services are holding back its rapid growth. The challenge for the industry is to scale up the security level of these networks to provide protection and peace of mind to everyone involved as the continued worldwide dependency on the service increases.

Physical health is fundamental, particularly for medical practitioners but digital health and security is also key for the industry. Like health, it isn't good enough to be reactive to potential issues that could prove dangerous, being proactive and shielding patients from data risks will prevent reputational damage to organizations and telehealth itself. Remote doctor appointments are here to stay and this isn't just because of a social distancing need but because it represents a more convenient and efficient way for patients and practitioners to complete appointments. Ensuring that this service is always safe and secure will see the technology flourish in the future new normal for telehealth.

The cybersecurity prognosis for the industry is to do anything that increases the digital health and therefore, security of your organization's IT infrastructure.

Kaspersky's experts share the following recommendations on the steps which medical institutions should take to protect themselves and their patients:

- **Endpoints are the main target for cyberattacks.** Ensure that all corporate devices which have access to the company's network and the internet are protected. This includes computers, office smartphones, tablets, terminals for recording, information kiosks, and medical equipment.
- **Regular software updates are the best way to eliminate the opportunity for adversaries to use old unpatched vulnerabilities as initial attack vector.** Unfortunately, in some cases organizations have to use equipment with legacy OS due to compatibility issues or high cost of upgrades. In this situation use security solutions optimized for unsupported operating systems. Kaspersky Embedded Systems Security delivers multiple layers of essential security technologies (including application and device control, anti-malware and network protection) to protect embedded systems from the latest threats.
- **Security awareness of employees is essential to ensure the safety of an organization and the data it possesses.** Ensure that all workers, including medical staff, know about cyber-risks and understand how to confront them. Employees also need to have a clear idea of cybersecurity measures implemented in their organization and be able to explain to patients how their personal information is protected.
- **A healthcare company must have an email security solution – healthcare organizations receive a lot of emails, including spam.** Unfortunately, spam often contains dangerous attachments that can harm the company's infrastructure.
- **Cybercriminals use a wide range of methods in the hunt for personal information.** Weak passwords provide them with an opportunity to steal sensitive data. Implement a strict password policy including multifactor authentication and identity and access management solutions.

Cyberthreat news: securelist.com
IT security news: business.kaspersky.com

kaspersky.com

kaspersky