CODE DIGITAL:

WILL HEALTHCARE THRIVE OR SURVIVE

WILL HEALTHCARE THRIVE OR SURVIVE
WILL HEALTHCARE THRIVE OR SURVIVE
WILL HEALTHCARE THRIVE OR SURVIVE

WELCOME NOTE

Since 2022, research conducted by SOTI demonstrates how global healthcare organizations have struggled to keep up with the pace, cost and complexity of modern mobile technology. There is still a backlog of technology projects from the 2020-2022 pandemic, and 13% of organizations continue to use legacy systems.

Despite the need for digital transformation within the industry and an overarching understanding of how technology can transform the space, this report outlines that the sector has remained stagnant over the past two years while calling out what is needed to move forward.

Research shows that the main concerns relate to IT support and the advancement of existing technologies to keep pace with modern demands within the healthcare sector. Healthcare organizations need to ensure that security is a priority to enhance global patient care, and address data breaches and compliance risks.

The inability to manage new and broadening technologies in legacy infrastructures has led to three key issues shared by respondents:

1. **Security:** Data privacy issues for patients and organizational data remains at risk.
2. **Innovation:** Transitioning to future technology is a struggle due to legacy systems.
3. **Telehealth and AI:** The absence of remote monitoring prevents the industry from fully leveraging these advancements.

Shash Anand, SVP, Product Strategy

The aim of digitizing the healthcare sector should be to build a technology ecosystem where devices and healthcare technologies are integrated and managed into the next era of innovative patient care.

Instead, as many as 20% of IT professionals say their biggest area of concern is spending too much time fixing small issues rather than focusing on transformative projects that assist frontline healthcare workers to provide the best care possible.

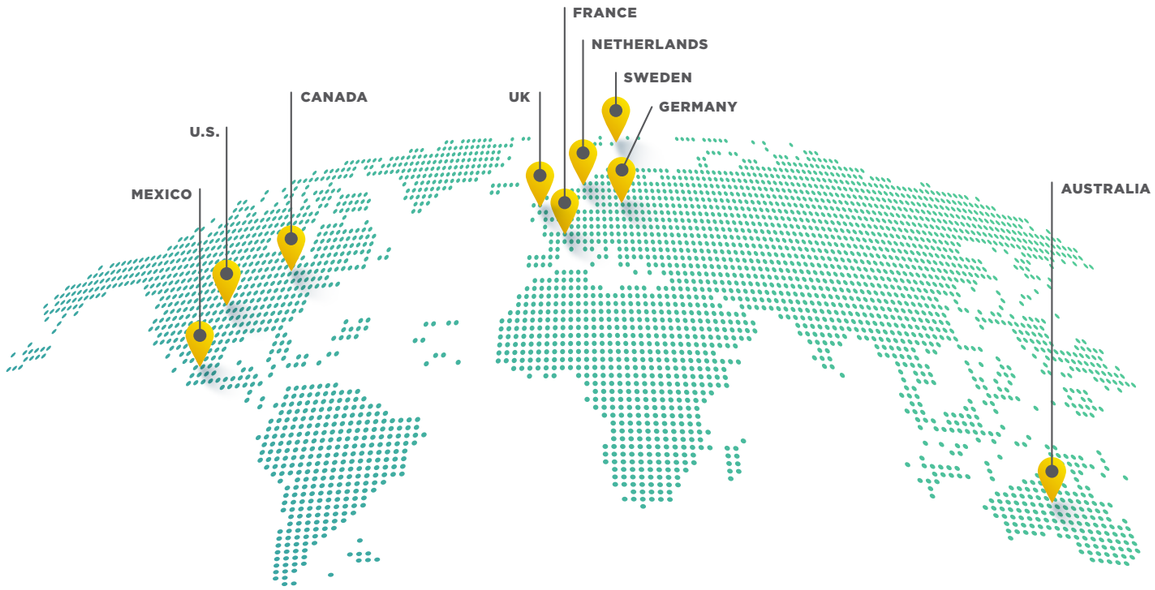
Despite this, technology investments in healthcare have increased since 2022, but confidence in the current condition of IT infrastructures seems to have diminished. Healthcare is still at a stage where devices – and therefore health data – are still not tracked and managed effectively. Issues are not automatically flagged and remote patient care is not enabled due to a lack of security and trusted data.

In this report, we dive deeper into the three overarching concerns, security, innovation and telehealth and AI. We explore why intent around tech is not leading to action, where excitement for the future of the industry exists and what is needed from an IT infrastructure standpoint to move the industry forward.

CONTENTS

METHODOLOGY

SOTI's research spanned 1,450 IT decision makers across the U.S. (200), Canada (150), Mexico (150), UK (200), Germany (150), France (150), Sweden (150), Netherlands (150) and Australia (150). The fieldwork took place between March 7 and March 25, 2024. All respondents worked within the healthcare industry in either a hospital, general medical practice, clinic or an organization that provides direct-to-patient remote or telehealth services.



GLOBAL BREAKDOWN

Overall, one-third (**32%**) of IT professionals interviewed worked in a general medical practice or clinic either within doctors' surgeries, as a family doctor or in a medical practice.

A further **25%** worked in clinics providing frontline patient services across one or more fields, including mental health, neurology and physiotherapy.

Other represented roles include those working in hospitals providing frontline patient services (**24%**) and healthcare professionals providing direct-to-patient remote or telehealth services (**18%**).

GLOBAL FINDINGS

86%

A resounding majority believe their organization would benefit from **better interconnectivity of devices.**

85%

A vast majority believe **new or better tech is needed to improve patient care.**

85%

A majority believe **AI could help simplify tasks,** but only 23% are currently using AI widely at present.

71%

Almost three-quarters of respondents globally are **transferring data to external hard drives/backup when disposing of old devices.**

67%

More than two-thirds of organizations **experience regular problems with IoT/telehealth devices** leading to patient care delays.

45%

All forms of **cyber incidents have been experienced** more in 2024 than a year ago, with both data breaches (33% in 2023) and accidental data leaks (38% in 2023) up to 45%.

63%

Almost two-thirds confirm **they are using outdated technologies now,** rising substantially from 46% two years ago.

23%

Data security concerns have risen back to 2022 levels (24%), which is up from 16% last year to become the number one IT issue.

3.9 hours per week per employee

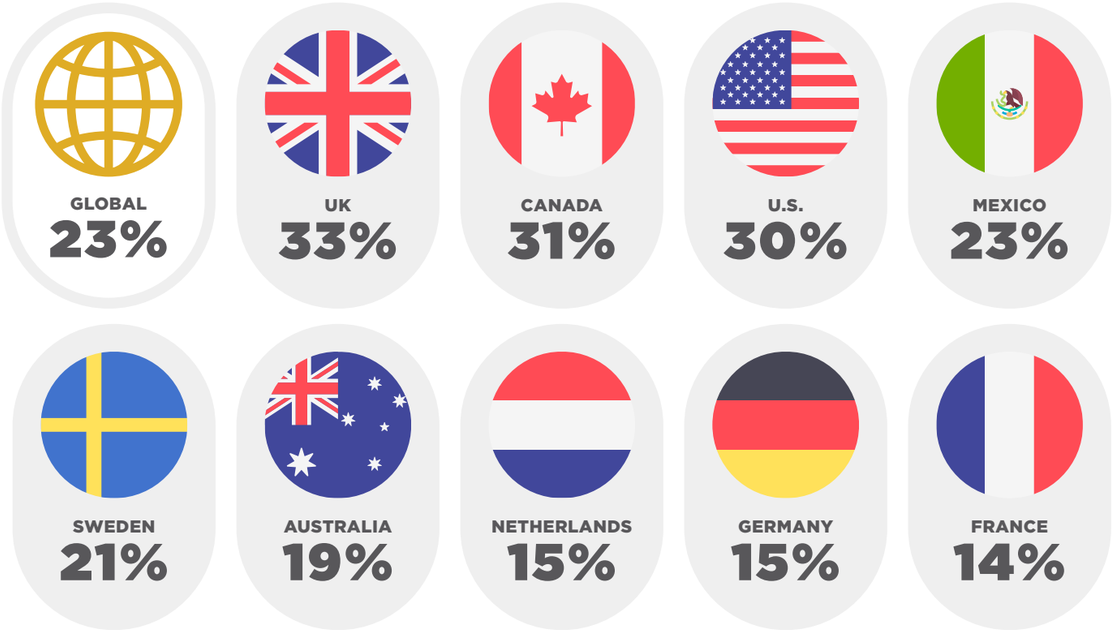
Legacy tech is contributing to an increase in lost hours due to downtime, rising from 3.4 hours last year.

DATA SECURITY

PATIENT PRIVACY & PROTECTING DATA

When it comes to IT, **23%** stated that data security was their most pressing concern. While this is fewer than one-quarter, it was still the most common answer and, concerningly, takes us back to 2022 levels (24%) when organizations were recovering from the pandemic. It is also far higher than in 2023 when only **16%** globally cited data security as their number one issue.

‘Data security is currently the biggest area of concern for IT within my organization’:



The UK (**33%**), Canada (**31%**) and the U.S. (**30%**) were most likely to list data security as their main IT concern.

What are your biggest concerns, if any, about the security of patient records held digitally within your organization?

Patient records could be stolen in a cyber-attack	42%
Reputational damage of a breach	38%
Financial costs of a breach	37%
Data is not adequately backed up to the server or cloud	36%
Patient information could be revealed without consent	36%
Patient information could be lost	34%
Lost or stolen devices revealing patient information	33%
Unauthorized access to patient records	32%
No training to keep patient records safe	23%

When asked about the potential effects of a cybersecurity incident, nearly all possibilities were listed as a concern by more than one-third of respondents.

However, **42%** expressed the main concern is that patient records could be stolen in an external cyber-attack, which is similar to 2023.

HIGHEST
LEVEL OF CONCERN

U.S. **50%**

UK **49%**

CANADA **46%**

LOWEST
LEVEL OF CONCERN

NETHERLANDS **37%**

FRANCE **37%**

GERMANY **29%**

The second highest concern was reputational damage, which increased from 34% in 2023 and 2022, to **38%** this year. This blend of data security concerns and associated reputational hits becomes more of an issue when respondents reveal the extent of data lapses from outside sources (**12%** increase), accidental data leaks by staff (**7%** increase) and ransomware attacks (**7%** increase):

Security issues organizations have experienced since 2022:

	2023	2024
Accidental data leak from an employee	38%	45%
Data breach from an outside source	33%	45%
A DDoS ransomware attack	30%	37%
Planned data leak from an employee	30%	34%

Based on this table, data security should be a higher concern than it is, with all forms of experienced breaches, attacks or leaks increasing since last year.

Security issues organizations have experienced by country:

	Data breach from outside source	Accidental data leak from employee	DDoS ransomware attack	Planned data leak from employee
	45%	**45%**	**37%**	**34%**
	40%	41%	33%	22%
	51%	63%	24%	46%
	50%	46%	38%	40%
	32%	33%	30%	15%
	38%	47%	40%	44%
	46%	43%	33%	42%
	47%	47%	40%	41%
	55%	53%	52%	34%
	43%	44%	38%	34%

While the extent of incidents differs from country to country, the Netherlands (**55%**) is a standout case study, with the country experiencing the most data breaches from an outside source and the most DDoS ransomware attacks (**52%**), yet only **15%** of respondents from the Netherlands currently list data security as their main IT concern.

Germany also tops the global average in three of the four security incident categories despite only **15%** placing data security as their main IT concern.

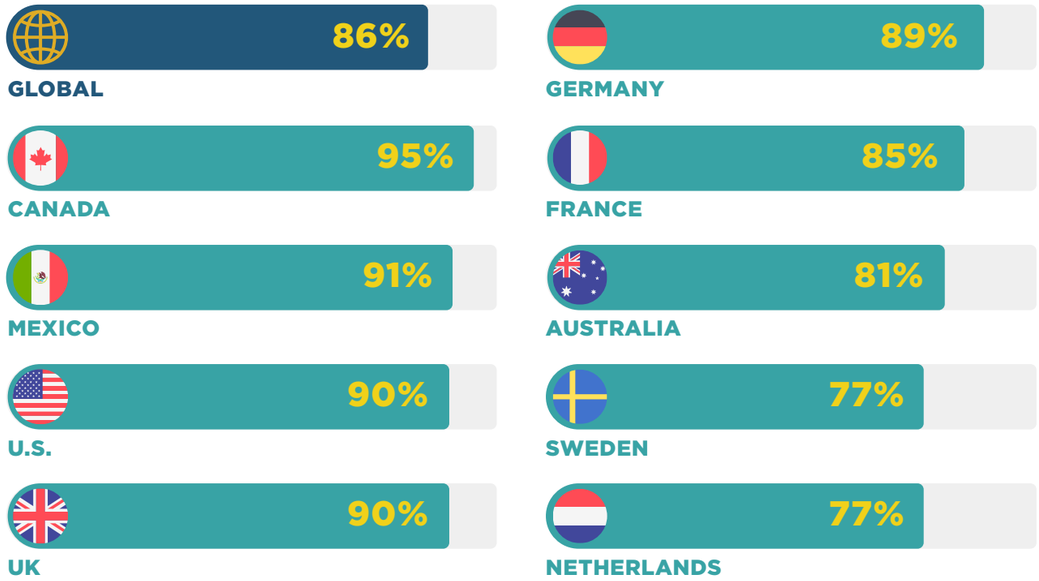
Canada faces the largest extent of both internal and external data leaks, which aligns with their heightened concern around data security (**31%**).

Globally, the sharp increase of attacks and leaks has risen quite drastically from 2023, however this is not reflected by many countries' concerns surrounding data security. Whether this is because of other focuses and priorities distracting organizations from the issue is unclear. However when the listed outcomes are so severe, affecting both the organization and patients' private information, it is quite surprising that security is not more of a central concern when discussing IT.

DEVICE INTERCONNECTIVITY: SHARING AND CARING

Sharing devices in healthcare settings is common. The vision of desktops on wheels being passed between physicians is familiar. The boundaries between each worker relate to their personal login credentials, which can create security vulnerabilities around personal and patient data. The management and visibility of these devices – who has accessed them, from where and for what purpose – without encroaching on patient privacy is critical. This is even more so when devices become interconnected between staff to provide more seamless and timely patient care.

Nearly all respondents believe their organizations would benefit from having more interconnected medical devices for patient healthcare:



When asked whether the management of shared devices was their biggest concern, only **12%** agreed.

On a positive note, the intent around using interconnected devices is evident across the board and offers huge potential, if organizations can ensure devices are properly managed, updated, secure and working properly during shifts.

THE DISPOSAL DILEMMA

Encouragingly, **100%** of organizations are currently taking measures to protect patient data when disposing of old devices.

The measures taken include:

Backing up patient data to the cloud — **51%**

Transferring patient data to an external drive — **40%**

Overwriting patient data with new software/data — **37%**

Hiring a third-party recycling company to manage the process — **36%**

Removing the hard drive and keeping it — **32%**

Erasing the hard drive — **28%**

Deleting patient data — **26%**

Measures your organization takes to protect patient data when disposing of old devices:

	Transfer to external hard drive/backup	Delete/overwrite patient data	Remove/erase hard drive
	71%	**54%**	**51%**
	74%	50%	43%
	74%	55%	49%
	71%	53%	42%
	72%	45%	40%
	69%	59%	60%
	69%	51%	57%
	58%	55%	53%
	69%	65%	64%
	79%	61%	56%

The importance of effective device management becomes clear when discussing the issue of lifecycles and effective disposal.

Most organizations are neither deleting data nor erasing hard drives when disposing of devices, and this creates risk. The instinct in healthcare will be to keep and transfer patient data to new systems, and the use of the cloud to ensure safe passage of this data is encouraging (**51%** globally – the most frequent measure taken).

However, if the transition is not managed effectively, then that surviving data becomes vulnerable to leaks and unauthorized access.

Organizations seem stuck in a middle ground of either keeping data but not trusting their ability to keep it secure during a system changeover, or deleting the data and creating more work for colleagues and strain on patients to rebuild their medical profiles.

Sitting between those concerns is the need to gain better visibility of devices so that their disposal can be planned ahead of time. An expert integration partner can help to ensure secure and seamless data transfers without the need to delete critical patient information.

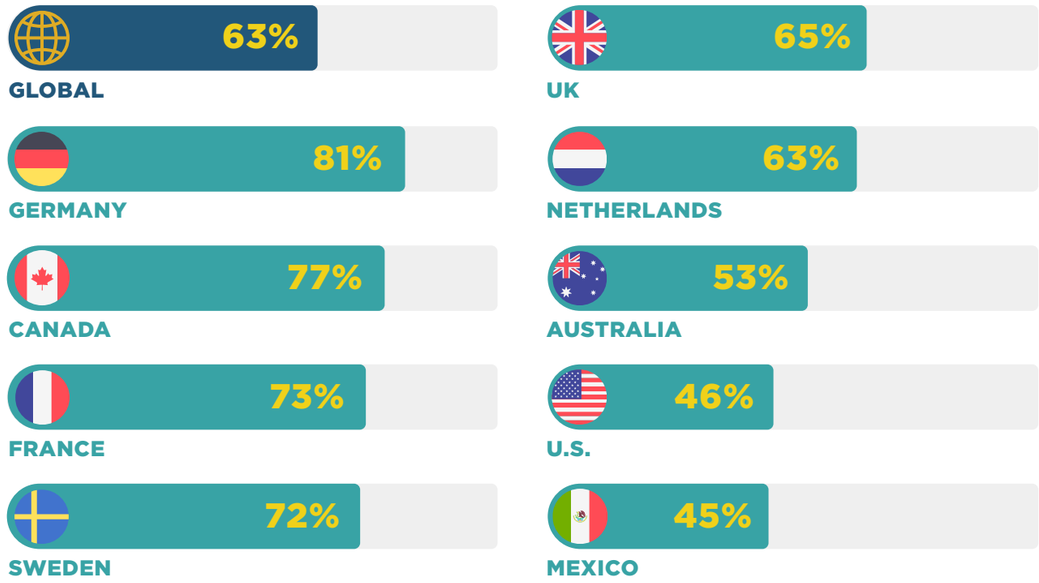
PATIENT CENTRIC INNOVATION

IN WITH THE OLD, SLOW WITH THE NEW

Healthcare organizations need to manage their transition away from legacy tech in order to be innovative. For example, hospital staff need to collect and retrieve information on their devices as well as be able to access Electronic Health Records (EHR) in the palm of their hands. They need new and integrated technology to allow for better management of devices, security of devices and to troubleshoot device issues in real-time when they arise.

If technology integration is lacking and processes are not updated, then the transition from old to new will meet resistance by healthcare organizations and staff. Healthcare workers are currently working with outdated technologies, with Germany at the top (**81%**), followed by Canada (**77%**) and France (**73%**).

‘My organization is using outdated technology’:



These insights into global legacy technology helps to explain why data security might be the biggest concern for healthcare IT decision makers. It also points to other bottlenecks in the healthcare sector such as how outdated tech impacts the ability to share information seamlessly, speed up and ensure better levels of care, enable remote patient monitoring and make hospital workers' jobs easier.

The most telling statistic of all is comparing responses around outdated technologies from 2022:

'My organization is using outdated technology':

2022
46%

2024
63%

Global healthcare professionals are using less fit-for-purpose solutions than they were just two years ago and this comes with significant consequences:

- **This year's respondents report an average of 3.9 lost hours per week, per employee, due to technical or system difficulties. This is a rise from 3.4 lost hours in 2023.**
- **More than a quarter (26%) lose over five hours a week, compared to 19% in 2023.**

ADOPTING MODERN SOLUTIONS, ABANDONING LEGACY TECH

When respondents were asked about the impacts of legacy tech on their organizations, they pointed toward various issues that would cost workers time and effort, while also potentially harming patient care.

What impact does legacy IT have on your ability to modernize your day-to-day operations?

37%
Spending too much time fixing issues.

36%
Making networks vulnerable to security attacks.

31%
Inability to access patient data quickly.

Spending too much time fixing issues:

GLOBAL	37%
MEXICO	36%
NETHERLANDS	49%
AUSTRALIA	35%
CANADA	44%
GERMANY	30%
UK	38%
SWEDEN	30%
U.S.	38%
FRANCE	28%

The Netherlands (**49%**) and Canada (**44%**) once again come out on top, confirming their previously stated concerns around tech management relating to downtime and legacy issues rather than security.

Across the board, more than one in three organizations are actively trying to fix issues caused by outdated tech. Combining this key concern with a similar statistic around those who are unable to access data quickly (**31%**), the impact on patient care becomes clear.

One in four (25%) respondents confirm they cannot deploy or manage new devices, which is up from 21% in 2023.

When asked about the prospect of investments into innovation, the responses highlight frustration around new technology investments:

85%

My employer needs to invest in new or better technology to improve patient care.

My employer needs to invest in new or better technology to prepare for a future health crises.

85%

82%

My organization has increased annual spending on technology since the start of COVID-19.

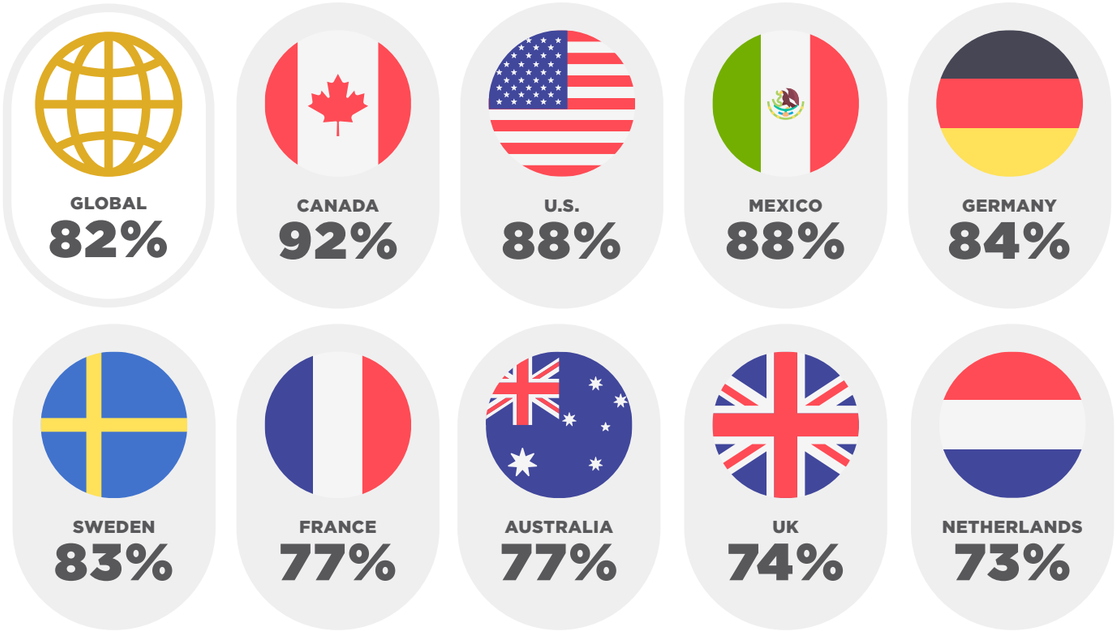
Although tech investments have increased since 2020, **85%** of respondents agree that their healthcare employer needs to invest in new or better technology to improve patient care. This implies that the wrong investments in tech are being prioritized, or that they are not being made with enhanced patient care in mind.

For example, alleviating administrative burdens from healthcare staff and clinicians, and introducing digital forms and more widespread automation, such as the improved use of applications, can enhance the exchange of information between healthcare teams and devices.

The vast majority of respondents feel that by failing to innovate or integrate and manage new technologies effectively, patient care is not as good as it could be and they are left more exposed to a future health crisis.

On a positive note, the benefits of new technologies can be identified once they are integrated and most importantly, managed effectively.

‘The technology (e.g., tablets, smartphones, scanners, RFID readers) my organization has provided me to do my job helps me do it faster’:



Across the board, there is an awareness of the potential that new tech could have on enhancing day-to-day tasks. However, the gaps identified in technology infrastructure further demonstrate the challenges the industry faces when it comes to advancing its digital footprint. For example, drilling down into device performance, having visibility into battery levels to avoid downtime, understanding why problems occur and being able to troubleshoot those issues remotely are capabilities the industry should have to meet the needs of today’s digital innovation landscape.

Additionally, enhanced security features to lockdown, encrypt and geofence devices should be the status quo for an industry that handles sensitive patient information. The key is to find a better roadmap and engage with technology partners that can help migrate away from outdated legacy tech, avoid hours lost from fixing device issues and move toward a more efficient and productive system for both staff and patients.

TELEHEALTH AND AI

REMOTE MONITORING FLATLINES IN REACHING ITS FULL POTENTIAL

Telehealth (also known as telemedicine) refers to the provision of healthcare using technology to communicate, update patient records and monitor patient health digitally, making care more efficient. It is therefore concerning and surprising that currently **24%** of organizations globally cannot support devices remotely.

This shortfall explains why healthcare professionals cannot make the most out of telehealth opportunities. For those that do, it explains why **67%** of respondents report regular problems with IoT/telehealth medical devices, leading to delays in patient care:

GLOBAL	GERMANY	CANADA	FRANCE	SWEDEN
67%	81%	79%	73%	73%

UK	NETHERLANDS	U.S.	AUSTRALIA	MEXICO
70%	61%	59%	57%	52%

Germany (**81%**) and Canada (**79%**) continue to share their struggles with digital transformation and managing newer forms of healthcare tech, but all countries reported more than **50%** agreement with telehealth device issues.

This **67%** global figure is higher than in 2022 when only 53% experienced regular problems with telehealth devices. This could be because the proliferation of devices in the sector has grown, but it still suggests in relative terms that organizations are unable to manage the transition or introduce more advanced, interconnected solutions.

In general, **89%** of those working in telehealth said that their organization would benefit from more interconnected medical devices. For example, collecting data from wearable mobile health devices, such as smartwatches that monitor heart rate, activity levels and blood glucose, where data can then be automatically uploaded to a patients electronic medical record.

Although these Remote Patient Monitoring (RPM) solutions exist, the report shows that managing this data integration is a challenge and provides even further confirmation that the infrastructure and management processes are not where they need to be to realize the full potential of telehealth and telemedicine.

The idea that the industry is struggling so greatly with the most basic forms of telehealth is particularly troublesome, especially when we take account of what the future of technology looks likes in terms of incorporating advancements such as AI and machine learning. Without a strong foundation that sets the standard for device implementation, visibility, management and security, imagining a future of even more interconnected and advanced tech seems dismal.

AI: A SHOT IN THE ARM FOR TELEHEALTH

If integrated effectively, AI and machine learning remove some of the current bottlenecks in telehealth. This type of tech would help to provide a more seamless connection between patient and physician. It would automatically and more accurately update patient records, and produce quicker, automated treatment plans that would be visible to those patients digitally.

With that, it is reassuring that 98% of all organizations have at least considered using AI in patient care.

Almost two-thirds (61%) confirmed AI was already being used to some extent.

- **Rising** to **80%** in Mexico, **72%** in the U.S. and Canada, **71%** in Germany, and **70%** in Australia.
- **Falling** to **47%** in the UK, **45%** in France and **43%** in the Netherlands.

Nearly one quarter (23%) went as far as to say AI was being used widely across its organization.

- **Rising** to **39%** in Germany, **35%** in Canada and **29%** in the U.S.
- **Falling** to **13%** in the Netherlands and Mexico, **15%** in the UK and **19%** in France.

Almost one-quarter working in telehealth are struggling to convert AI intention into AI investment. This suggests the lack of a clear roadmap or understanding of how to elevate remote-care processes with AI.

When asked how AI is currently helping their organizations with patient care, respondents listed:

- **Processing or analyzing medical data** — **60%**
- **Updating patient records** — **56%**
- **Planning treatment courses** — **47%**
- **Personalizing treatments** — **44%**
- **Diagnosing conditions** — **38%**
- **Administrative purposes** — **20%**

More than half (**59%**) state they are anxious about using AI in patient care. This could be because its benefits are not yet familiar and normalized. We can infer this based on the following responses about AI's listed benefits:

Using AI can:

85% **Simplify tasks**

Be a cost-saving strategy **83%**

83% **Reduce human error**

Compared to 2022 when 72% agreed AI helps to simplify tasks, that global figure now sits at **85%**, with this rising to **88%** among telehealth personnel.

Overall, **81%** of respondents believe most medical staff in their organization would support the use of AI in patient care. Unsurprisingly, this rises to a high of **86%** among those working in telehealth or associated sub-sectors.

Though still in its early stages, the telehealth sector faces challenges integrating new solutions for optimal remote care. **Respondents highlight AI as the key to accelerating telehealth's progress and unlocking its full potential**.

UNDER THE MICROSCOPE:
BREAKING DOWN BARRIERS TO DIGITAL TRANSFORMATION

Globally there is an understanding of technology's potential and how it can transform patient care, staff satisfaction, process speeds, accuracy and security in the healthcare sector.
The report shows that there is often a plan and budget in place to help spark digital innovations, improve device connectivity and create a more seamless administration of remote care.
Furthermore, there is an alignment of how innovations such as AI could transform organizations.

Where organizations seem to be falling short is knowing how and when to make their first move, how to successfully integrate new technologies into their organization and how to manage devices effectively across its entire lifespan. Recurring challenges include the outdated use of legacy tech, transitioning to new solutions without security and privacy, device and hard drive disposals and failing to capitalize on new breakthroughs such as AI and automation.

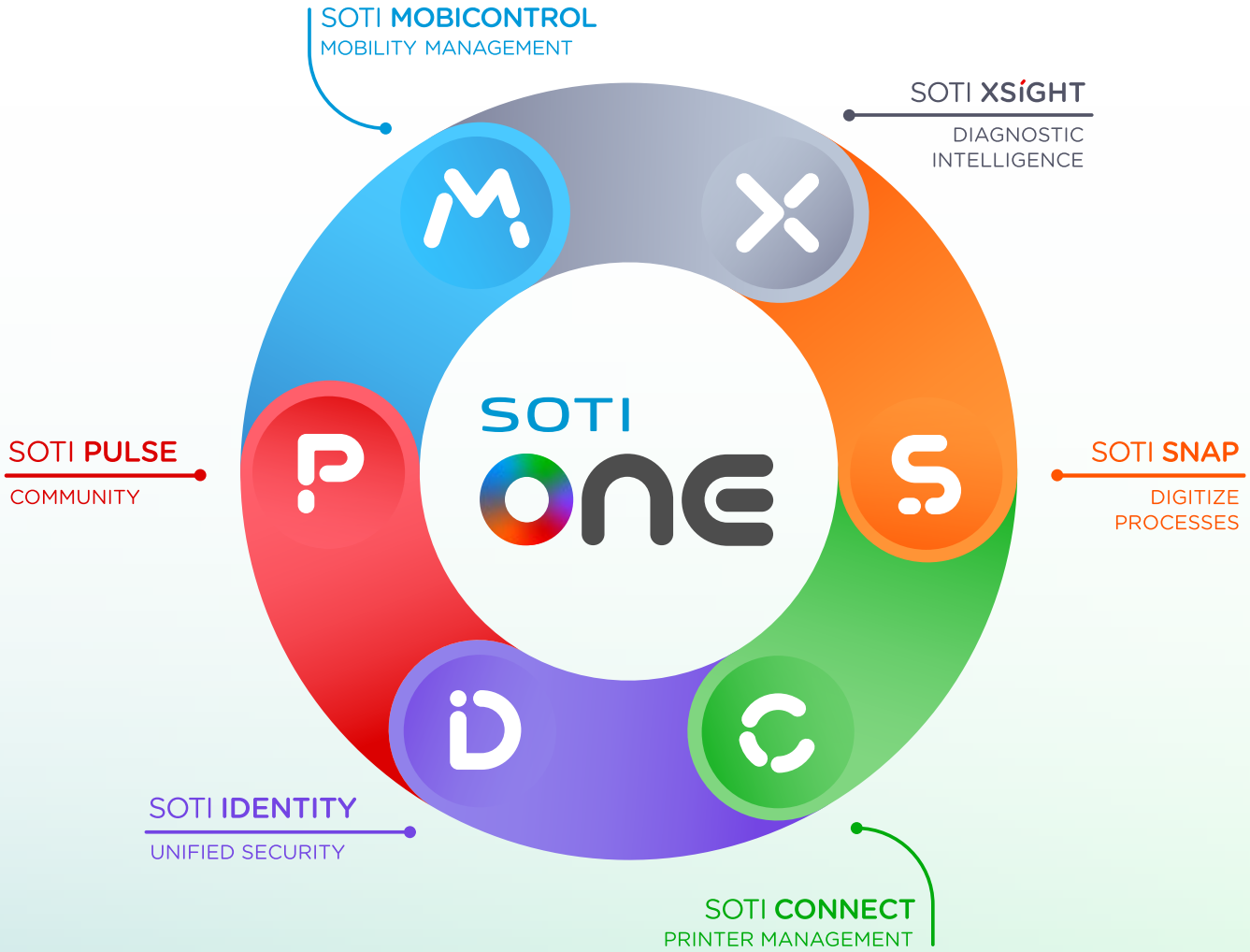
The need for more intelligent solutions to help guide the transition from old to new and to aid the integration process has been highlighted by this year's findings. When asked about the most pressing concerns, **62%** fall into a combined bucket of either data security concerns, spending too much time fixing small issues, managing the security of shared devices or experiencing legacy tech issues. Knowing where, when and how frequently these device issues occur and being able to identify and fix them remotely would be a major step forward to speed up patient care and free up IT time managing smaller IT problems.

AI, RFID readers, rugged devices, wearables, chatbots and a host of new technologies alongside burgeoning sectors such as telehealth will continue to evolve at a rapid pace. The intent is to help healthcare keep up with them, however in reality the industry is still in the early stages of its digital transformation journey.

Now that we understand the needs of the industry, the key is to determine the right tools and technologies to build a digital transformation roadmap and support these organizations to excel in the future of patient care.

ABOUT SOTI

SOTI is a proven innovator and industry leader for simplifying business mobility solutions by making them smarter, faster and more reliable. With SOTI's innovative portfolio of solutions, organizations can trust SOTI to elevate and streamline their mobile operations, maximize their ROI and reduce device downtime. Globally, with over 17,000 customers, SOTI has proven itself to be the go-to mobile platform provider to manage, secure and support business-critical devices. With SOTI's world-class support, enterprises can take mobility to endless possibilities.



TO LEARN MORE:

For additional information on how SOTI can set your business up for success, **click here**.
To learn more about the SOTI ONE Platform, **click here**.
To find out how SOTI can help with your mobile investments, contact us today at **sales@soti.net**.

SOTI is a proven innovator and industry leader for simplifying business mobility solutions by making them smarter, faster and more reliable. SOTI helps businesses around the world take mobility to endless possibilities.

soti.net

052424