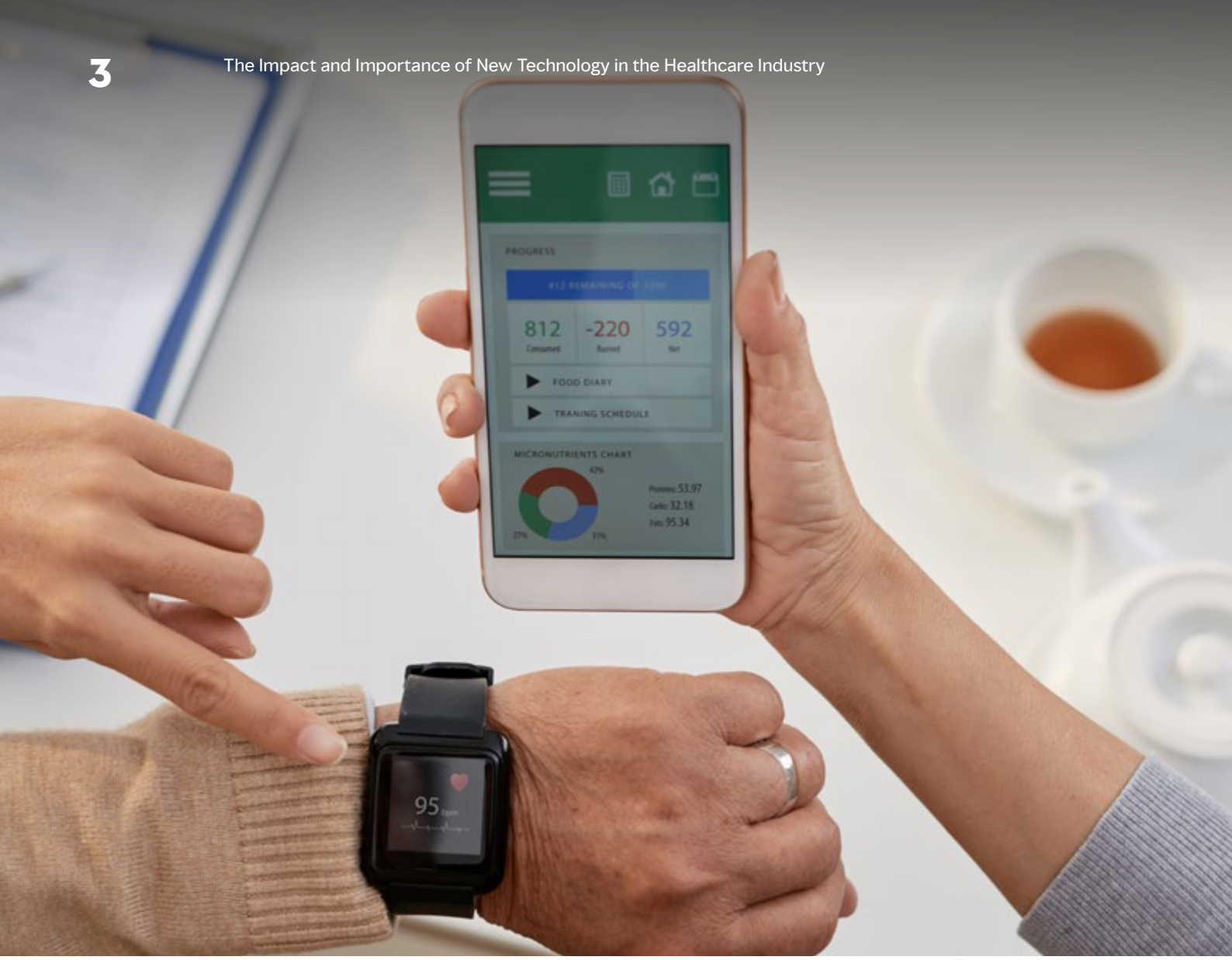
Marsh Commercial

The Impact and Importance of New Technology in the Healthcare Industry

Care sector insights

An evaluation of the risks and benefits associated with new technologies on your care business.

Contents



Abstract

Artificial intelligence and digital medicine are transforming the healthcare industry[1]. From saving time in administration, to improving patient health, the potential for healthcare technologies are endless.

But the introduction of new technologies in healthcare has not come without its setbacks. From breaches in data confidentiality, to questions of ethics, investing in new technologies can bring new and sometimes unprecedented risks. Risks which may even, arguably, outweigh the benefits.

So, what do these new technologies really mean for your care business? Can you afford to evolve with the industry? And how can you manage the risks if you do?

1 | https://www.goanywhere.com/blog/2018/02/06/2018-cybersecurity-concerns-in-healthcare

63%

NHS found that 63% of adults would be willing to have a video consultation with their GP for advice on a minor ailment.

New technologies in the healthcare industry

While it's hard to predict the future, there's no doubt that now is an exciting time for the healthcare sector. New technology has great potential for improving patient care. It could also have a huge impact on cutting costs and reducing pressure on staff and recruitment.

How future technologies are improving healthcare:

- More efficient administration
- Faster diagnosis
- Improved data security
- More personal treatment
- Safer practice
- Cutting costs

The following are some of the most popular and progressive new technologies already being used by the healthcare industry.

Technology for residents, service users and patients

Telemedicine

Internet of Things (IoT) and mHealth are the most widely used telemedicine technologies. Often connected to wearable devices, they're used to diagnose and treat patients remotely outside a hospital setting. The main function of the IoT is to collect data, giving doctors invaluable insight into symptoms and enabling remote care[2].

By giving access to virtual advice, Telemedicine can help people with dementia live in their own home for longer. Surrey and Borders Partnership NHS Trust together with health technology providers, have been providing individuals and their carers with sensors, wearables and monitors to give service users more control over their own health and help social care staff give more effective services[3].

The impact of Telemedicine on healthcare business

Telemedicine is transforming the treatment and diagnosis of disease[4]. While IoT offers insight into symptoms and trends[5], mHealth gives patients the ability to track and personalise their care. The mHealth apps sub-sector saw an annual growth of 35% between 2014 and 2018, making it the greatest healthcare investment in the last decade[6].

2 | https://econsultancy.com/internet-of-things-healthcare/

3 | https://iotuk.org.uk/wp-content/uploads/2017/11/IoT-in-Health-and-Social-Care.pdf

4 | https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/461479/BIS-15-544-digital-health-in-the-uk-an-industry-study-for-the-Office-of-Life-Sciences.pdf

5 | https://econsultancy.com/internet-of-things-healthcare/

6 | https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/461479/BIS-15-544-digital-health-in-the-uk-an-industry-study-for-the-Office-of-Life-Sciences.pdf

Wearable Devices

Wearable health monitors such as smart watches can provide real time data about the health and wellbeing of the wearer. They can track daily routines to determine when your service user will most likely need assistance.

They can also check vital signs including blood pressure and sugar levels, helping medical professionals in both diagnosis, treatment, patient monitoring and prevention of illness.

These are just some of the ways wearable devices are being used by patients to improve the quality of their healthcare:

- **Personalisation –** Through the use of new and improving software, doctors can quickly create personalised programmes based on the needs of the patient.
- **Early diagnosis –** By looking back at data stored by wearable devices, doctors can use their precise medical parameters to detect the early development of symptoms.
- **Remote monitoring –** Healthcare professionals are now able to monitor patients remotely, making their care more rounded and consistent and diagnosis more reliable.
- **Stored medical data –** With medical data being recorded and stored in real-time, doctors are able to achieve a more complete outlook of the patient's medical history.
- **Medication reminders –** Wearable devices can help patients remember when to take their medication. They can also alert medical professionals if medications are being abused.
- **Reducing costs –** Wearable devices allow for remote healthcare. This has the potential to save time in healthcare visits, and reduce the number of tests required to gain accurate diagnostics.

Other examples of wearable technologies include:

- Glucose monitors
- Cardiac monitors
- Body-worn sensors (used to detect symptoms for specific diseases such as Alzheimer's)

Alarms Systems[7]

Home and personal alarms systems are devices that activate a trigger response to a healthcare professional if a patient falls or has a problem at home. These systems are particularly useful for elderly or less mentally or physically able patients who live alone.

These are just some of the eventualities which could lead to a home alarm being triggered:

- A fall
- A fit or seizure
- A vulnerable patient wanders too far from home
- The patient or environment is too hot or too cold.

Alarm systems can range from watches, pendants, emergency buttons, pull-cords, or even intercom systems.

7 | https://www.nhs.uk/conditions/social-care-and-support-guide/care-services-equipment-and-care-homes/personal-alarms-security-systems-and-keysafes/

86% **A 2016 report from CB Insights found that 86% of healthcare providers are using a form of artificial intelligence technology.**

Technology for medical professionals

It's not only service users, patients and care recipients that can benefit from these advances in technology. They are also having an impact by improving standards of care, even on the surgery table, and are improving the success of treatments[8].

Wearable Devices for medical professionals

Wearables such as Google Glass with preloaded CT and X-Ray images are helping healthcare professionals in their day to day work by increasing efficiency and minimising human error[9].

An eyeglass headset accessed via a smartphone, Google Glass allows for hands-free computing, photo/video recording, directions, and data sharing. It also has a HD screen capable of recreating an image equivalent to 25 inches.

Below are just some of the ways wearable technology is starting to impact the medical profession:

- Providing easy, hands-free access to patient charts when away from the computer.
- Allowing for instant documentation and transcribing of notes, comments and conversations.
- Giving paramedics the ability to transfer accident information, photos and video clips to emergency rooms ahead of patient arrival.
- Faster retrieval of patient analytics (x-rays, MRI, etc.), with real-time document transfers.
- Remote assistance, enabling specialist guidance from medical professional working off-site.
- Allowing doctors performing surgery to simultaneously monitor a patient's vital signs, refer to x-rays and react to changes without putting the patient at additional risk[10].

Artificial Intelligence (AI) and Robotics

AI and Robotics are allowing healthcare professionals to carry out complex procedures with even more precision, flexibility and control. AI based coaching systems and data lead outcomes across various procedure scenarios can provide professionals with accurate training[11].

AI and Robotics can also provide automated staffing solutions. Automated roles can include anything from administration and virtual diagnostics to health monitoring systems, bridging gaps in the healthcare workforce[12].

The impact of AI and Robotics on healthcare business

Tasks such as patient administration and preliminary diagnostics can now be carried out by AI. By saving time and money on staffing, healthcare businesses are now able to maximise patient care at contact level.

8 | https://sightcall.com/wearable-tech-taking-healthcare-industry/
9 | https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5668637/
10 | https://www.meditek.ca/google-glass-healthcare/
11 | https://www.einfochips.com/blog/the-future-of-healthcare-iot-telemedicine-robots-artificial-intelligence/#readmore
12 | https://novatiosolutions.com/10-common-applications-artificial-intelligence-healthcare/

56% **In a recent study, IBM predicts that 56% of healthcare executives will employ Blockchain solutions by 2020[13].**

Digital Health Systems

Digital systems such as Electronic Health Records (EHRs) and Blockchain are used to store, link and move highly confidential data[14]. These technologies make patient records easier to access, helping improve both the quality of healthcare and patient confidentiality.

Electronic Health Records (EHRs)

An EHR is a digital version of a patient's paper medical chart. EHRs are kept and updated in real-time, making information available instantly and securely to all authorised users. They not only contain the medical and treatment histories of a patient, but the EHR system is specially built to go beyond standard clinical data collection as is typically available by a single health provider.

Some of the key features of EHRs are:

- They are able to compile a patient's medical history, diagnoses, medications, treatment plans, immunisation dates, allergies, radiology images, and laboratory and test results in one easily accessible space.
- They provide medical professionals with access to evidence-based tools which can be used to make decisions about a patient's diagnosis and care.
- They automate and streamline workflow, making data collection and storage more reliable and quicker to access.

However, the most useful feature of an EHR, is its ability to share data across multiple platforms instantly. By using EHRs, authorised providers can access and manage up-to-date patient health records in a digital format. These records can then be shared with other providers across multiple health organisations, including: laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics. With instant access to medical information from all clinicians involved, medical professionals will be able to provide a better standard of care[15].

Blockchain

Blockchain in healthcare, is an encrypted method of recording and storing medical systems and parameters. It also has the ability to analyse and action automated decisions based on these parameters.

Blockchain has huge potential in improving the medical manufacturing process, as well as monitoring shipments and dispensing. A key example of how Blockchain is used in the pharmaceutical industry, is its use in managing temperature control. Temperature control is vital for the safe storage and shipment of certain pharmaceutical products. With Blockchain, information can be tracked throughout the whole supply chain, with the information collated and recorded in real-time. The stability of the product can then be accurately determined before distribution.

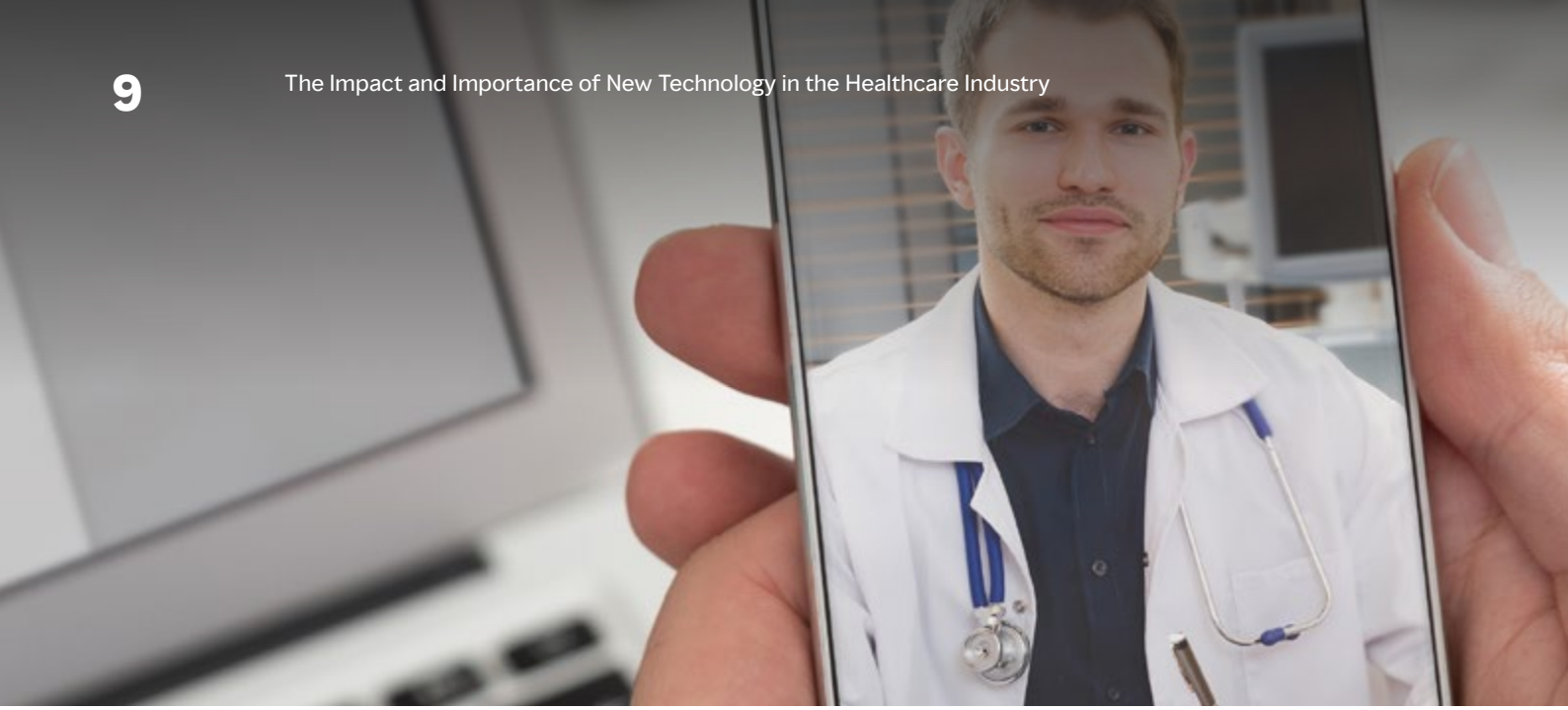
Other uses for Blockchain include the safe sharing of patient data during medical trials, and the tracking of prescription medicines.

Already widely used throughout the pharmaceutical industry, the technology is now being taken up by hospital and healthcare institutions[16].

How digital health systems are impacting healthcare business

Digital Health Systems provide a more secure way to store and manage data. These technologies provide a great opportunity to reduce costs by decreasing paperwork. They can also reduce the risk of medical errors, ensuring all information is up-to-date at the point of care[17].

13 | https://www.ibm.com/downloads/cas/BBRQK3WY
14 | https://www.pwc.co.uk/industries/healthcare/insights/how-blockchain-could-transform-healthcare-systems.html
15 | https://www.healthit.gov/faq/what-electronic-health-record-ehr
16 | https://www.ft.com/content/6f138722-47d4-11e8-8c77-ff51caedcde6
17 | https://www.healthit.gov/faq/what-are-advantages-electronic-health-records



What's next for healthcare technology?

The healthcare industry has seen some dramatic changes over the last few years, from manual to computerised records, developed population health tools and enhanced security. This rate of change isn't looking to slow anytime soon.

In November 2018, John Halamka (Professor and Chief Information Office at Harvard Medical School), made some predictions about future technology.

Below are five predicted changes that could impact your care business:

Cloud hosting is taking over

Rather than storing data in on-site data centres and local computers, cloud hosting is predicted to replace or partly replace this method.

Subscriptions to cloud based services means that hardware, project resource and time investment is hugely reduced. Applications that need a maximum data transfer rate which is easier to achieve with local hosting, will probably need a hybrid solution, at least for the time being.

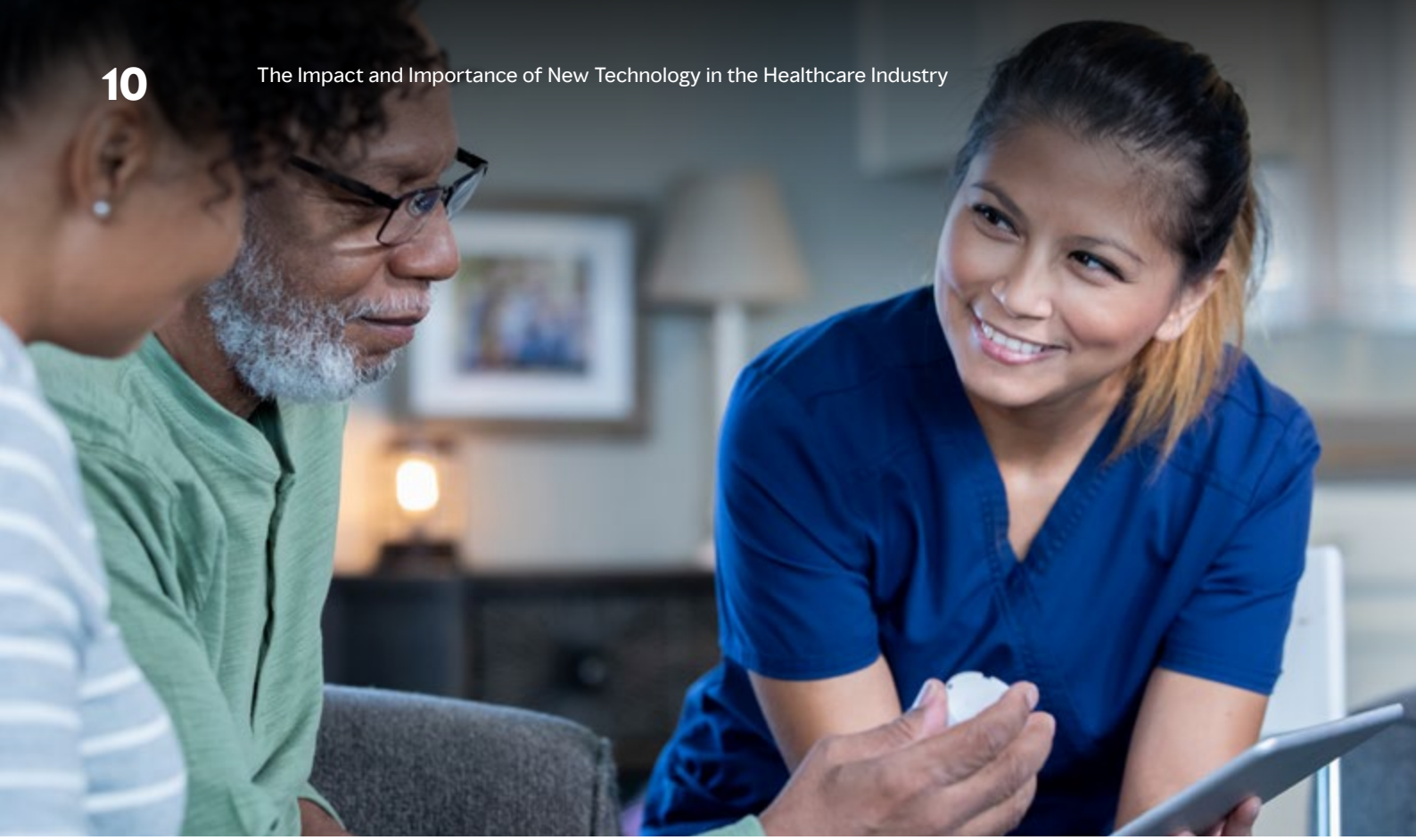
Services will be more mobile optimised

At Beth Israel Deaconess Medical Centre (BIDMC), 80% of all website traffic is now using a mobile device. Using the internet on mobile devices over desktop is a growing trend, and the healthcare sector is no exception.

Patients and care providers both want to be able to access the records they need, schedule services such as appointments and manage medications from their mobile device.

Login portals will be replaced with mobile apps that connect to the Internet of Things (IoT). Patients can then manage their health through reporting systems and by accessing their data.

Telemedicine technologies which are often connected to wearable and mobile devices will be used to enable remote care, and keep patients healthy in their home. This will disrupt the delivery of healthcare, similar to how Amazon changed the shopping experience.



Machine learning will use past data to optimise for the future

Machine learning will use millions of past patients' experiences to predict treatments for current patients.

Some examples of how machine learning can optimise patient experience are:

- Operating room scheduling
- Patient length of stay forecasting
- Predicting who's likely to not show for an appointment

The algorithms used in machine learning requires data to be very accurate and high quality. At present a lot of healthcare data has validity issues meaning that work is required to allow this new technology to work.

Intelligent voice recognition goes further

Intelligent voice recognition or ambient listening products such as the Amazon Alexa and Google Home, will be used more by healthcare organisations. In the UK, we have an aging population which is putting pressure on the care system.

These products have the ability to help reduce some of the strain and make patients' lives easier.

Healthcare organisations will be able to design skills and commands that interact with practice management systems, so booking a routine appointment can be done by voice command. We will even be able to use sentiment analysis to assess voice for mental health issues.

How Blockchain will help

New technologies rely upon consent for data sharing and patients must trust these applications. Blockchain can be used to hold patient's consent preferences, which can then be accessed by various applications.

Allowing flow of data whilst protecting privacy. Blockchain will also provide audit trails to track where the data is being used and the integrity of the record. As Blockchain is not a database it won't replace electronic health records (EHRs) but it will create trust by ensuring that data processing is secure and traceable.

+100m

In 2015, over 100 million healthcare records were compromised from more than 8,000 devices in more than 100 countries[19].

Analysing the risks

Evolving technologies bring new risks including cyber risk. Cybersecurity in the care services industry has been a growing concern over the past few years. And with the arrival of GDPR, fears about pitfalls could become more widespread[18].

In 2015, over 100 million healthcare records were compromised from more than 8,000 devices in more than 100 countries[19]. And this is only likely to increase with the growing interconnectivity of modern software and devices.

Some of the risks your business may face due to new technology are:

- Harm to a patient's safety and health by hackers accessing personal devices[20].
- Loss of SPI (sensitive personal information) by hackers accessing personal data from connected systems. In 2016 3.47m patient records were stolen from Newkirk Products[21].
- Breach and access of wearables and monitors which are susceptible to remote takeover[22].
- Ransomware on connected systems - the healthcare industry is the most affected by this with 34% of all ransomware attacks[23].
- Negative PR due to a data breach[24].

It's important when investing in new technology that you carry out the appropriate risk assessments. Your risk management strategy must be updated to allow for new working practices. Failing to do so could leave you open to claims not covered by your current insurance.

18 | https://www.goanywhere.com/blog/2018/02/06/2018-cybersecurity-concerns-in-healthcare
19 | https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/top-cyber-security-risks-in-healthcare/#gref
20 | https://iotuk.org.uk/wp-content/uploads/2017/11/IoT-in-Health-and-Social-Care.pdf
21 | https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time
22 | https://iotuk.org.uk/wp-content/uploads/2017/11/IoT-in-Health-and-Social-Care.pdf
22 | https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks
24 | https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time

65%

of Chief Information Security Officers in care services believe they have "inadequate in-house expertise" to deal with a cyber security breach[28].

The most common cyber threats for care service providers

Increase in technology

Information Systems Audit and Control Association research shows mobile devices (54%), cloud (50%), and social media (38%) as the most difficult technologies to secure[25].

Internet of Medical Things (IoMT) is one of the most recent and accepted advancements in medical technology. However, these are also one of the biggest threats of cyber risk[26]. As more of your processes to remotely access information, IoMT devices are not built with security features.

Ransomware is an example of a new and evolving data security threat which acts by breaching shared IT systems and preventing access. The cost of a healthcare data breach has been calculated at £300 per individual record, with an average of 30 records stolen per breach, making this one of the most lucrative cyber scams[27].

Limited investment in cybersecurity

65% of Chief Information Security Officers in care services believe they have "inadequate in-house expertise" to deal with a cyber security breach[28].

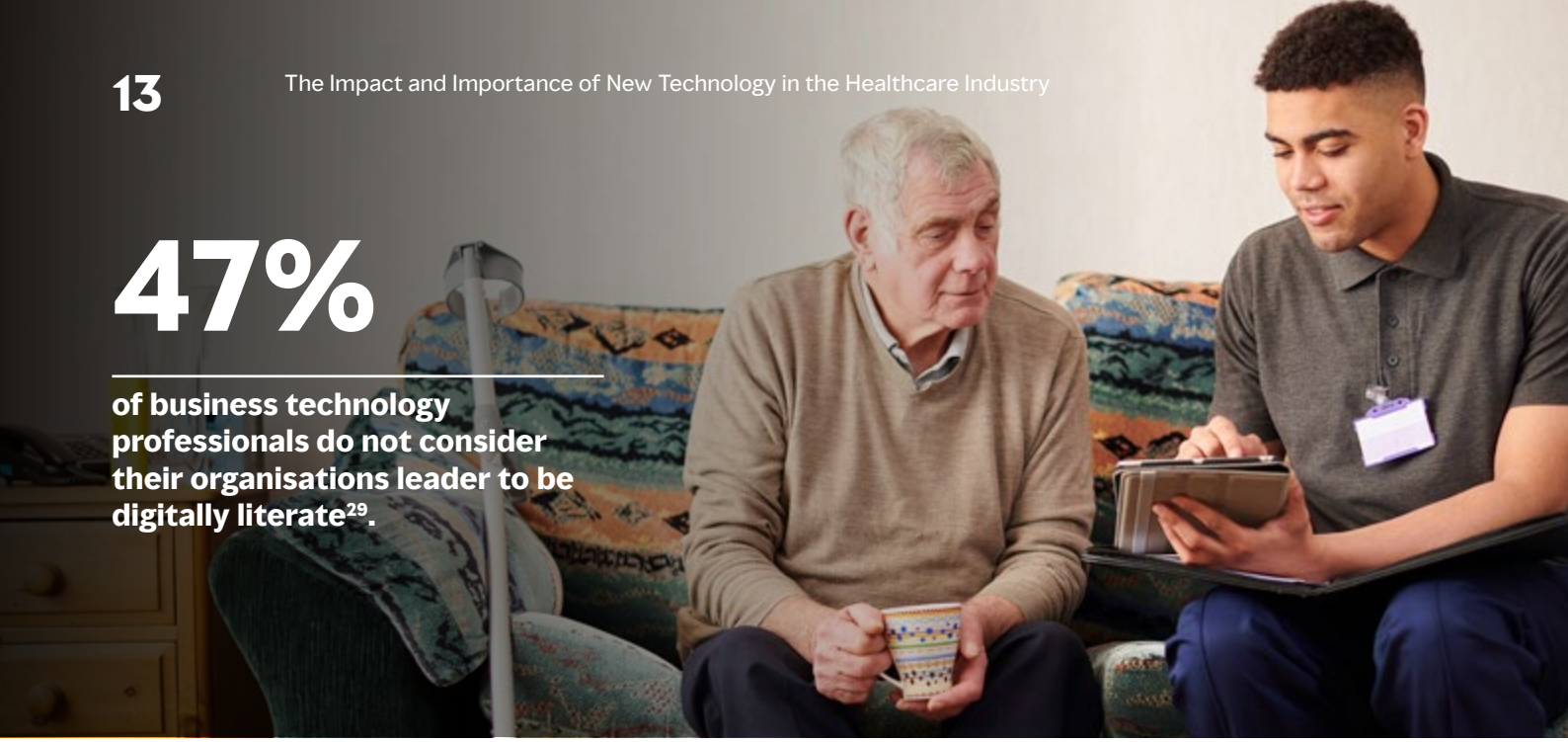
Cybersecurity investments in healthcare must compete with other more urgent needs. New medical technologies and equipment, staff and basic supplies are often your priority, potentially leaving your business unprotected.

Interconnectivity

Cybersecurity protection is particularly lacking in smaller and independent practices. If you're a small organisation, you might receive limited funding, which doesn't sufficiently cover your cyber security needs.

With modern technology, your business is more at risk than ever. The connectivity of the care services industry, makes your small business an easy way to breach larger organisations by accessing their data through your systems[28].

25 | https://healthitsecurity.com/news/iot-security-top-concern-for-business-technology-leaders
26 | https://www.fortinet.com/blog/industry-trends/minimizing-cyber-risks-as-healthcare-providers-increase-technology-use.html
27 | https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/
28 | https://healthitsecurity.com/news/67-of-cisos-believe-a-cybersecurity-attack-will-happen-in-2018



47%

of business technology professionals do not consider their organisations leader to be digitally literate[29].

Risk planning

How to tackle the risks posed by new healthcare technology.

Working in the healthcare sector, there are some unique risks posed by modern technology to your business that won't affect other organisations.

These include:

- Volume of personally identifiable information and health information stored on shared systems.
- Creation and transmission of Electronic Health Records (EHRs) and Personal Health Records (PHRs).
- Reliance on external service providers for payment processing and laboratory testing.
- Responsibility for risks posed by suppliers and third-party services.

Make sure that your healthcare business has appropriate risk management planning and care insurance in place to ensure you're adequately covered. Without it, the risks and associated cost of new technologies to your healthcare business, might be seen to outweigh the benefits.

Below are a few simple actions which could help protect your business against cyber threats:

Educate

Did you know that 47% of business technology professionals do not consider their organisation's leader to be digitally literate[30]?

Every member of staff, from doctors to administrators, play a role in keeping your organisation secure. But many are not aware of how their day-to-day activities might open the doors to a data breach.

Education for your staff is essential in protecting against CEO and dishonesty fraud. Your staffs' knowledge on what to watch out for and the processes in place if there is a cyber breach should be evaluated.

29 | https://www.calyptix.com/hipaa/10-biggest-problems-in-healthcare-cybersecurity/
30 | http://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/2017-Digital-Transformation-Barometer.aspx

Create a cybersecurity policy

A good cybersecurity policy is essential in managing security throughout your organisation. Over 60% of providers don't have an effective Identity and Access Management (IAM) policy in place, leaving them wide open to an external breach[31].

A good Cyber Liability policy should help protect your healthcare business by:

Taking action

A good cyber policy will react as soon as a cyber security incident is flagged. It should cover your liabilities on everything from media and data security to viruses and hacking.

Rectification

Your cyber insurance should also cover any additional costs that stem from your initial liabilities. This includes the costs of customer notifications, credit monitoring and legal fees.

Repairing the damage

In addition to hiring forensics to identify root causes of your security breach, a good cyber policy should also offer a cyber consultant to help mitigate damage to your business reputation.

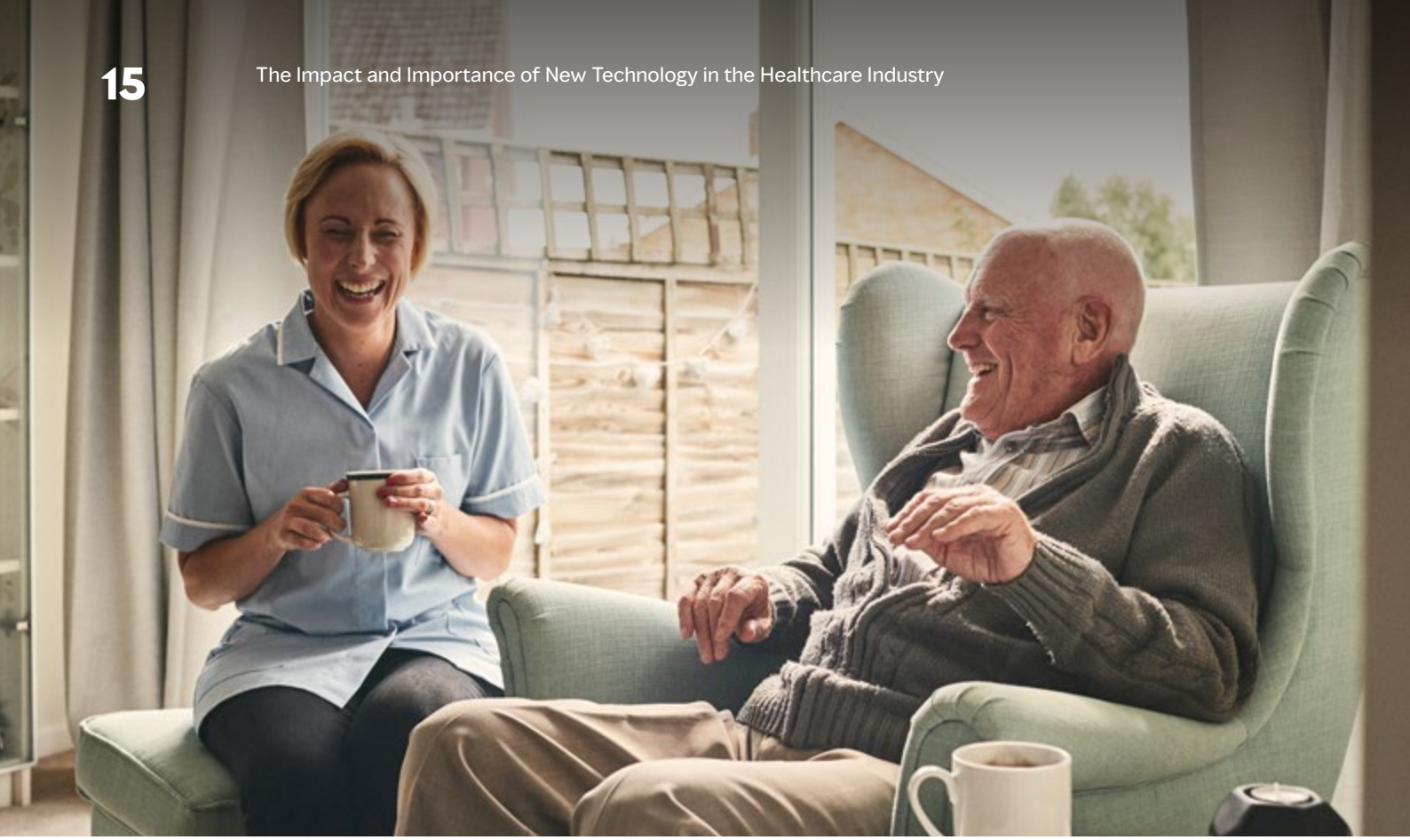
Carry out cyber threat assessments

A cyber threat assessment enables you to see how your staff are using applications. It not only helps ensure that cybersecurity policies are being followed, but improves compliance and patient data protection[32].

You should also assess the potential financial cost of a cyber-attack, build a model to quantify costs of a data breach and create an assessment for loss arising from data loss.

31 | https://www.goanywhere.com/blog/2018/02/06/2018-cybersecurity-concerns-in-healthcare

32 | https://www.fortinet.com/blog/industry-trends/minimizing-cyber-risks-as-healthcare-providers-increase-technology-use.html



Why your standard insurance policies won't protect against a cyber attack.

Though your existing policies may offer some level of coverage, they are unlikely to cover in the event of a cybersecurity breach.

Your basic insurance will usually cover:

General liability: covers injury and property damage, not economic loss.

Errors & omissions: covers economic damages resulting from a failure of defined services only - excluding data and privacy breaches.

Property insurance: covers tangible property only.

Crime: covers employees and tangible property. Offers no cover for third party property, including customer/client data.

Your basic insurance doesn't usually protect you if you're the victim of a cyber-breach. Having cyber security cover will help you with disaster recovery, should a breach happen.

Cyber insurance

Cybercrime is constantly evolving. New technologies bring with them new and unprecedented risks.

However, a comprehensive cyber insurance policy should promise to cover your business for all cyber related liabilities as well as managing any long-term fall out.

For comprehensive cyber insurance cover, look for a provider who promises to cover all of the following eventualities:

Regulatory defence and penalties

Your policy should cover payment for amounts which you are legally obliged to pay as a result of a civil regulatory action, regulatory compensatory award, civil penalty, or fines (as insurable by law), imposed by a government or public authority regulator.

Cyber extortion

Your policy should cover expenses incurred by you and your business, including the value of any ransom paid for the purpose of terminating a cyber-extortion threat.

Data breach notification

Your policy should cover the cost of consumer notifications following a data breach, to comply with data breach law. This includes legal fees, costs to send and administer notification communications, as well as the costs of call centre services to respond to enquiries and queries following a notification communication.

Business interruption

Your policy should cover you for loss of business income resulting from the total or partial interruption, degradation in service, or failure of information and communication solutions.

Fraudulent Representation

Your policy can cover payment for loss of the insured's money, property, products, goods, services or other financial benefit, where such losses are as a direct result of a fraudulent electronic communication designed to impersonate the partners, directors or members of the insured.

Talk to the experts

Marsh Commercial offer various Care Insurance packages to care services professionals as well as Cyber Liability Insurance to help protect your organisation against the risks posed by cyber security.

If you would like support in managing your risks, contact our expert Care Insurance team who will be able to help.

Marsh Commercial

For more information visit:

marshcommercial.co.uk/for-business/care

Or call our Health and Care team on:

0113 350 8712