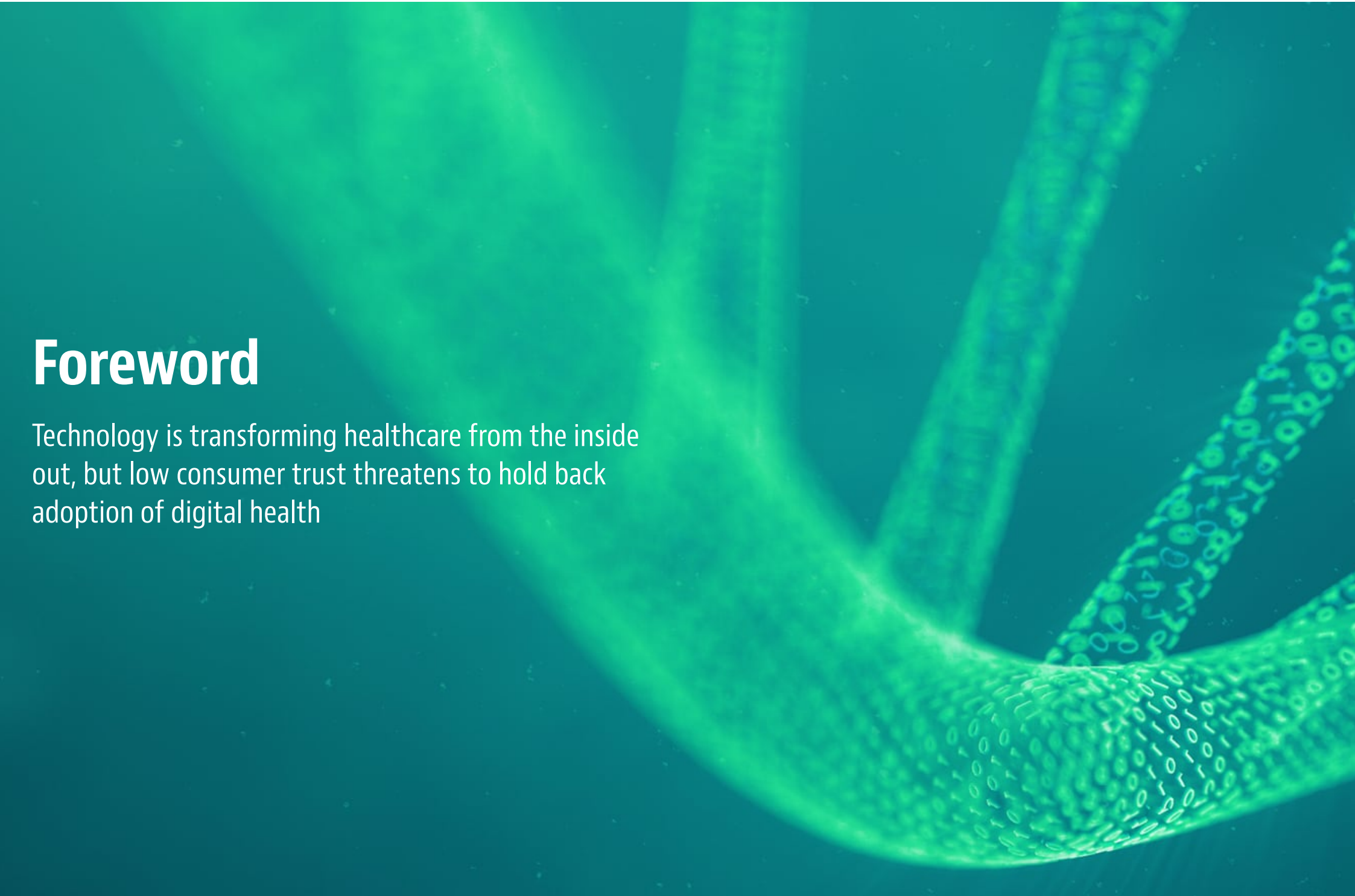
Baker McKenzie.

Outside The Comfort Zone

Building consumer trust in digital healthcare

Baker McKenzie.



Foreword

Technology is transforming healthcare from the inside out, but low consumer trust threatens to hold back adoption of digital health

Foreword

Technology is transforming healthcare from the inside out. More than ever before, digitisation of the healthcare ecosystem will put the patient at the centre of care – offering the promise of greater efficiencies, lower costs and enabling more precise treatments and therapies. The healthtech industry is booming, and pharmaceutical and medical device businesses are partnering with data specialists to offer new solutions to patients, and harness the data produced in a 'virtuous circle' of innovation.

But unlocking the benefits of digital health depends ultimately on consumer engagement. The industry needs patients to use technology and allow their experiences and outcomes to be used to support innovation and understand how diseases can be prevented and treated.

It is in this context that Baker McKenzie commissioned new research into consumer attitudes and concerns in relation to digitisation and data. The report combines robust, independent research with the perspective of our lawyers in London and globally on some of the drivers and challenges for the advancement of digital health.

Our survey results show that consumers are hesitant to adopt new technologies, especially those targeted at diagnosing, treating and monitoring conditions. When it comes to their data, many are also unclear as to who has access to their information and how this data is being used or shared, and despite new personal data security regulations under the EU General Data Protection Regulation (GDPR), few feel confident with the legal protections currently in place.

As a result, many respondents are being more selective about what information they will share and what digital health products and apps they will use. A significant proportion of consumers are becoming less, not more, willing to embrace digital health.

The root causes of mistrust are hard to pinpoint and consumer worries in this area are many and varied. Interestingly, the different concerns expressed, along with the motivations to share data, manifest themselves in different ways between demographics. Therefore by understanding and tailoring messaging and products to the attitudes of a particular target group, it should be possible to increase support for, and adoption of, transformational digital healthcare.

Ben McLaughlin, Chair of the Global Healthcare & Life Sciences Group, Sydney

Baker McKenzie.

A sceptical view on digital health

Consumers mistrust technology in healthcare

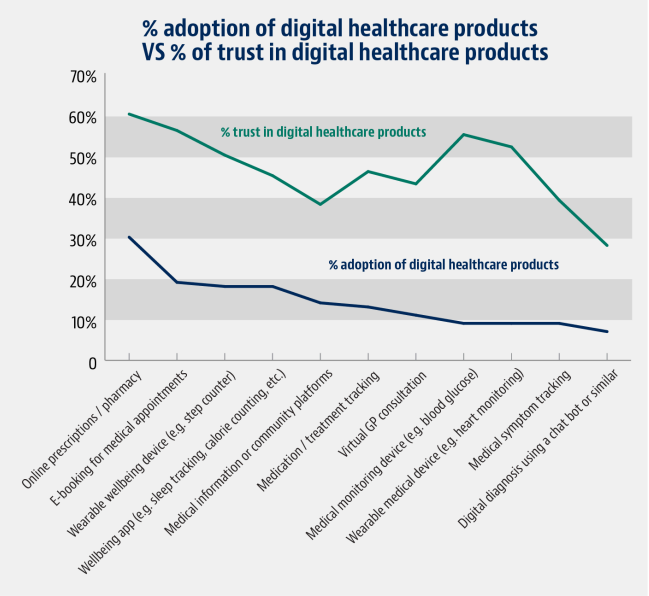
A sceptical view on digital health

Consumers take comfort in the familiar when it comes to their healthcare – a professional they can see and trust or a system that they know.

According to our research, traditional healthcare approaches are preferred to digital healthcare products in the consultation (60%), diagnosis (58%) and treatment (62%) of medical conditions for the majority of consumers.

The most popular digital health products are e-prescription services and e-booking for medical appointments, but even then, only 30% and 19% of consumers respectively, have used these within the last 12 months. Less than half of consumers (47%) trust digital health products overall, and unfamiliar, game-changing technologies like algorithmic diagnosis tools are treated with particular suspicion. Only 7% of consumers are comfortable using them and 13% plan to do so in the next 12 months.

Further, they remain unconvinced that digital health products can advance healthcare or deliver better outcomes for patients. Less than half (48%) of consumers agree that digital health is good for patients, while nearly two thirds (57%) of consumers think that digital health applications should be confined to administration and not care.



"Technology and health represent two different worlds. While the tech sector is known for its open source culture and speed of innovation. In healthcare introduction of new treatments is heavily regulated and patient confidentiality is a central tenet of healthcare delivery. It is not surprising as these industries have started to overlap that tensions have emerged."

Hiroshi Sheraton, Partner, London

Misalignment and complexity: Regulating digital health

There is little connection between the digital healthcare solutions consumers trust and the extent to which these are regulated.

Our data shows that consumers happily use and trust simple digital healthcare products that do not technically qualify as medical devices, such as well-being apps, which are subject only to general product regulatory standards, but could reasonably have access to sensitive information about medical history, geo-location, behaviour and test results. Meanwhile, digital healthcare products relating to medical diagnosis, treatment and monitoring, which constitute regulated medical devices, are among the least trusted by consumers, but must adhere to the highest standards of regulation.

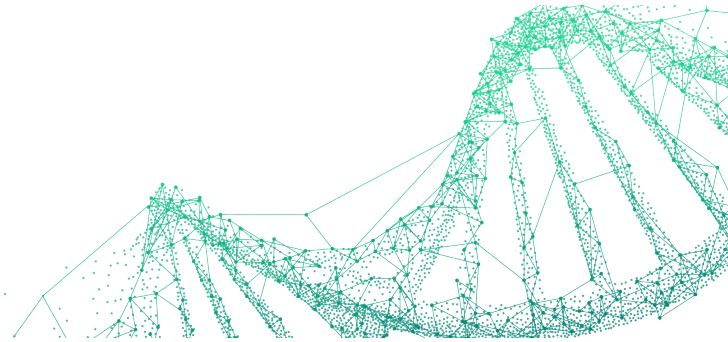
Complex digital healthcare software applications are typically treated as one of the higher risk classifications of medical devices under EU law. In the UK, under the European legislative framework, the Medicines and Healthcare products Regulatory Agency (MHRA) oversees and classifies medical devices to ensure they adequately protect patients and data. The EU-wide CE marking system (which the UK is likely to adhere to post-Brexit, even if it develops a UK parallel system) provides visual evidence of compliance with safety and efficacy standards.

By contrast, relatively unregulated lifestyle and well-being apps are generally regulated as standalone software in the same way as in any other sector. The borderline between medical device apps and well-being apps is not always clear. Certain permutations of functionality, promotional claims, and indications of the manufacturer's intent, are among factors that affect whether an app crosses that line and constitutes a highly regulated medical device.

Of course, the fact that the regulation tightens on more complex and risk-laden digital healthcare products is only right and proper. Indeed, the higher levels of scrutiny that such products attract, to ensure safety and efficacy, and the ongoing monitoring and surveillance they face in relation to adverse events including data security issues, are necessary to protect patients.

However, regulators have begun to take action to further tighten their oversight in this area. Under the forthcoming EU Medical Devices Regulation, which the UK is to implement regardless of Brexit, some health apps will be reclassified into higher risk classes, and others will be treated as medical devices for the first time.

Julia Gillert
Senior Associate, London



Baker McKenzie.

The heart of the matter

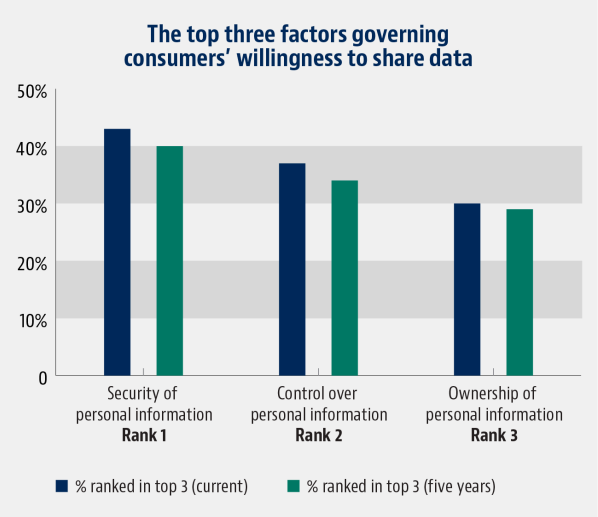
Data security concerns drive mistrust of digital health

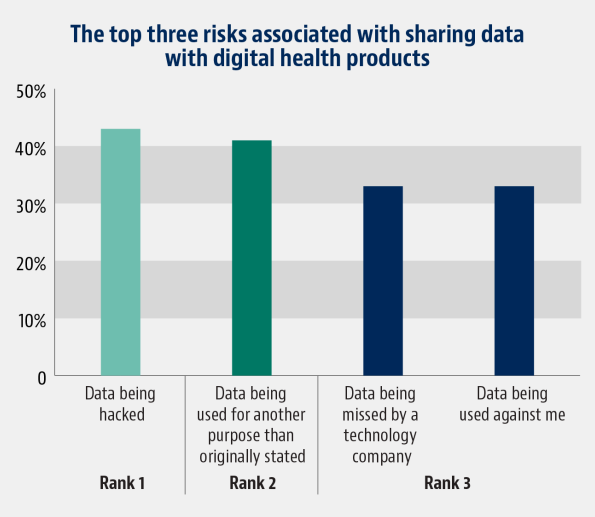
The heart of the matter

That less than half of consumers trust digital health products correlates with significant concerns they express about data security.

Our survey shows that consumers consistently rank data security among the top risks of engaging with digital health products. More than half of our respondents (54%) are concerned that their data will fall into the wrong hands, or could be used against them, for example, in the form of higher insurance premiums or employer discrimination. These concerns may be well-founded: two in ten (22%) consumers are aware that their personal information has been hacked.

Consumers also seem to lack crucial knowledge in relation to how their data is used and shared. 70% of consumers admit to being unclear on who has access to their information and just one in ten understand how their data is used or shared in relation to digital healthcare. Existing legal protections are not allaying these consumer concerns – just one in ten (11%) are fully confident in the legal protections in place to secure their data.





"Getting data security right is paramount. Nearly two thirds of consumers would consider litigation over mismanagement or poor protection of data – leading to a potential wave of small scale actions against digital healthcare companies. While pharma and medtech may be able to manage this within the existing mature legal infrastructure, one costly lawsuit could be the end for fledgling healthtechs, to say nothing of the reputational damage to the organisation and product, and the digital healthcare industry overall."

John Leadley
Partner, London

Clamping down on data breaches

We've seen consumers are deeply concerned about data security, but the existing legal framework already sets out a robust framework for addressing these concerns. Data privacy compliance and enforcement will now be key in building consumer trust.

The GDPR has been the biggest update to data protection regulation in Europe for two decades. It lays out a range of new rules and clarifications governing privacy across sectors, some of which have a significant impact in healthcare. Greater understanding of these guidelines, and how they seek to support privacy, should have a positive impact on consumer trust.

Demonstrating that breaches will be punished is key to this endeavour. The GDPR sets out obligations on data controllers and data processors to ensure the security of processing personal data, by implementing appropriate technical and organizational measures such as encryption, pseudonymisation, and regular system testing. It also builds in tools to protect data subjects, such as the concept of data minimization, which is the legal requirement to only use and collect the minimum data needed to fulfil the defined purpose.

The most serious breaches of the GDPR come with the potential for fines of up to €20 million or 4% of annual global turnover. The UK's Information Commissioner's Office recently handed down one of its largest ever fines at the time to Bounty – a company that provides information packs and goody bags to new mothers in maternity wards – for selling the personal data of millions of mothers and their new babies to up to 39 credit agencies and marketing groups. These mothers hadn't been properly informed of the sharing, and individual records were often sold to multiple customers, in some cases up to 17 times. Bounty was fined £400,000. Importantly, the ICO issued this fine under the previous data protection regime (the Data Protection Act 1998), which capped fines at £500,000. If this fine had been issued under the GDPR, it could have been a lot higher.

Jaspreet Takhar
Associate, London

The global perspective on data security in digital health

"Russian regulators place a high priority on data protection consent, but outdated processes mean it is difficult for companies to comply and compete. In practice, paper consent via a statutory form, countersigned by the patient or other qualified signatory, is required to authorise the use of health data. Similarly, copies of patient records must also be made onshore before these can be transferred or assimilated into international datasets. This could hold back digital health innovation, limiting international collaboration on treatments for global health priorities."

Sergei Lomakin
Partner, Moscow

"Asia is perhaps the least homogenous global region when it comes to regulating digital healthcare, and these fragmented regimes are creating significant complexity for healthtech. How best to manage regulatory divergence given that digital health products are borderless by design is a difficult question facing companies in the region and globally."

Dr Isabella Liu
Partner, Hong Kong

"Approaches to data and privacy are increasingly considered a brand issue for US companies. Accordingly, firms are reconsidering their calculus when it comes to data compliance, and are working to build and implement comprehensive programmes in spite of the complexity caused by different laws and standards."

Amy de la Lama
Partner, Chicago

Data as IP: Spotlight on Intellectual Property

Development of the digital healthcare industry has brought the value of data into sharper focus. Data was once a static collection of relatively low value information.

However, rich and active datasets now underpin digital healthcare products and represent a renewable source of value to pharma and medtech companies. As new data is collected and new pathways are drawn between data points, so value grows. To comply with data protection rules and optimise data interoperability, pharma and medtech companies often acquire data from third parties and outsource data processing to specialist companies. These organizations gather raw, siloed datasets and transform them into anonymised, harmonised ones – the essential groundwork that enables new digital healthcare products to be developed.

But when the value of digital healthcare is increasingly linked to the value of data, traditional concepts of intellectual property break down and it becomes important to distinguish between IP rights (arising from copyrights, database rights, know-how and patentable inventions) from concepts of ownership, control or access to data including information resulting from processing that data. That can lead to a complex network of multi-party agreements all of which must be consistent with data protection obligations.

The ability to recognise, allocate ownership of, and ultimately control the "value" generated as a result of using digital healthcare will depend on developing new flexible models for dealing with IP. This presents a huge challenge to the pharmaceutical and medical devices industries as the business models must adapt to structures more familiar to the big technology players.

Hiroshi Sheraton
Partner, London

"Healthcare is a highly acquisitive sector – buying up innovative medtech and biotech companies is critical to industry strategy and ability to bring new products to market faster. Healthcare accounted for as many as eight in ten M&A deals last year and healthcare M&A activity is predicted to reach $600 billion this year. As a result, data increasingly sits at the heart of deal value. With large amounts of sensitive information changing hands, companies are exposed to significant risk – from data protection and compliance issues to ownership and consent. Navigating these issues under tight timescales is critical to maintaining consumer trust as new partnerships are forged."

Jane Hobson
Partner, London

Baker McKenzie.

Regaining control of data

Mistrust leads consumers to withhold data and reject digital health

Regaining control of data

Consumer mistrust poses a serious threat to the sustainability of the digital health sector, and could slow the adoption of transformational products and services.

Fears about security and the knowledge gap on how their personal information is used is driving two thirds (65%) of consumers surveyed to seek to 'regain control' of their personal information. As a result, these consumers say they plan to become more selective about what digital health products they use – withholding data wherever possible as a means of exercising some control over their healthcare. Four in ten consumers say they already choose not to engage with digital healthcare due to data security concerns, and this is set to become more pronounced in the future. Just 8% of consumers say they will become more comfortable sharing personal information over the next five years and 20% will become less willing to engage.

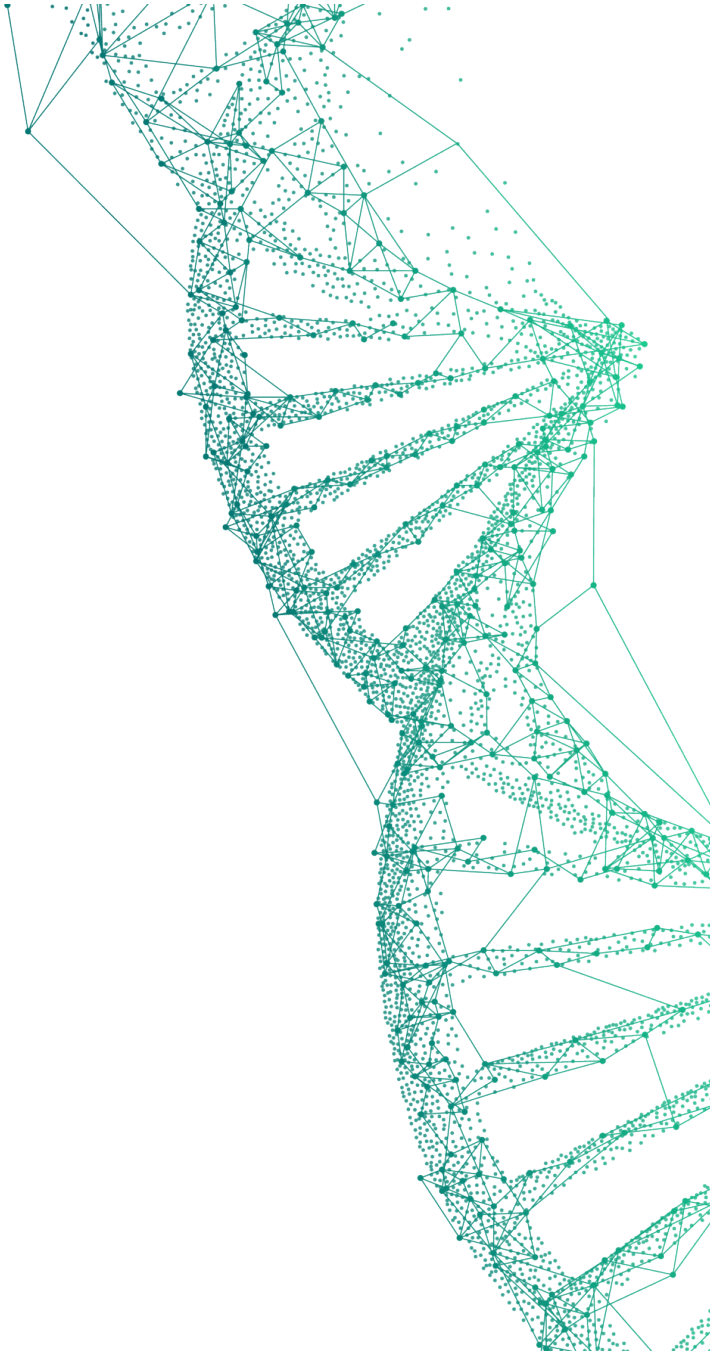
Improving consumer trust in digital health is therefore one of the most important steps companies operating in the healthcare ecosystem can take today to shore up future success. It is also important if the UK government's plans to reap the benefits of digital health are going to be realised.

8%

of consumers say they will become more comfortable sharing personal information over the next five years

20%

will become less willing to engage



Critical condition: Realising digital health opportunities in the NHS

The UK government sees the further development of digital healthcare as critical to meeting the future healthcare needs of the country, and managing the costs involved in meeting those needs. Over the last year there has been a plethora of policy announcements on this topic:

- in October 2018 the Department of Health and Social Care published its policy paper on the future of healthcare, setting out their vision for digital, data and technology in health and care;
- in February 2019 the government created NHSX, a new joint organisation for digital, data and technology to take forward digital transformation in the NHS; and
- in August 2019 the Health Secretary announced a £250 million investment in a new National Artificial Intelligence Lab to use the power of artificial intelligence to improve the health and lives of patients.

A key part of building trust will relate to the handling of patient data in connection with the development of digital healthcare. Building digital healthcare solutions, and in particular the deployment of machine learning and artificial intelligence, requires access to data on a large scale. The NHS holds the types of large scale real-world data assets that are needed for this, but our survey suggests the NHS will need to exercise care in how it seeks to deploy those assets in order to build and maintain public support.

There are measures already in place that address many of the consumer concerns we found in our research. For example, the NHS is prohibited from using patient data for marketing or insurance (unless a patient requests this) and – following the National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs in 2016 – the government introduced a number of measures intended to bolster the security of patient data. These included the adoption of the 10 data security standards set out in the National Data Guardian's review, a redesign and update by NHS Digital of the Information Governance Toolkit to support the new security standards, and the inclusion in the NHS Standard Contract of a requirement for organisations to implement the National Data Guardian's recommendations on data security.

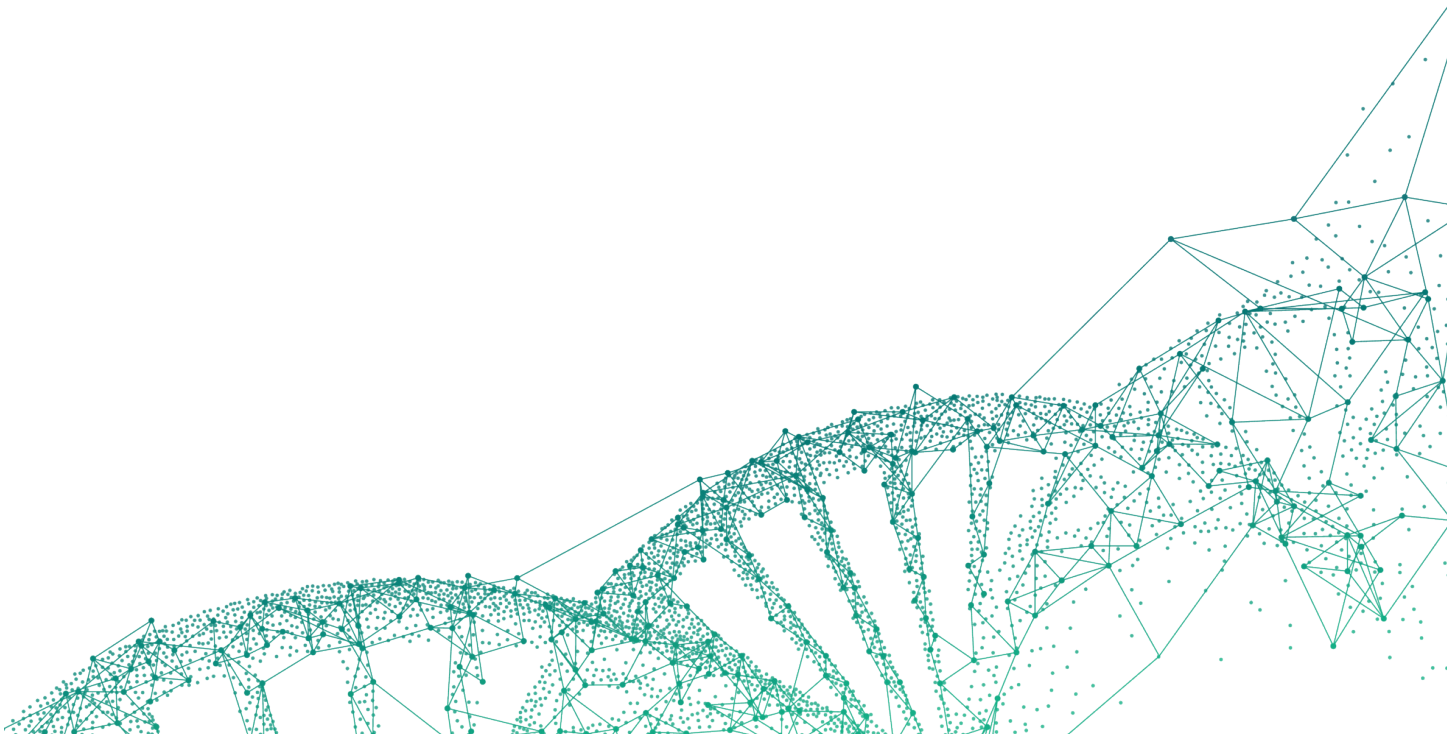
While perhaps more could be done to communicate the measures and prohibitions that are already in place, our survey suggests that it is not sufficient to provide only reassurances that patient data is securely held and will not be used against patients. There is a real need to improve the level and quality of information being provided around data sharing and use of patient data. The Wellcome Trust's Understanding Patient Data initiative has recognised the need for a more nuanced explanation of how patient data can be used (including how many applications access only particular aspects of the data on a patient on a de-identified basis rather than accessing all the patient's data).

Our findings also indicate that there may be benefits in tailoring information on this topic for different parts of the patient population.

This need for improvement in the level and quality of information provided around data sharing is important, not only to build consensus and buy-in around digital healthcare provision generally, but also because (following the National Data Guardian review) it is now NHS policy to give patients a national data opt out. Under this arrangement, they can opt out of their data being used beyond their direct care, such as to plan and improve health and care services and to research and develop cures for serious illnesses.

Importantly for the development of digital healthcare solutions, the opt out does not apply to anonymised data that meets the Information Commissioner Office's standards for anonymisation. However, these standards can be hard to meet in practice and, in any event, the use of anonymised data will not be appropriate for some digital healthcare solutions. Even quite low levels of opt outs can present problems for the development of digital healthcare, particularly if they occur in certain population groups, as this can lead to some demographics not being appropriately represented in studies, or the needs of particular groups not being properly taken account of in planning for healthcare needs.

Duncan Reid-Thomas
Partner, London



The challenge of data 'ownership'

Nearly two thirds (61%) of consumers say they want to regain 'ownership' of their data. Yet ownership is a difficult idea in relation to health information – individuals don't 'own' their medical records in the same way as they might a house or a car. But legislation does seek to empower consumers to exercise control over their data. To this end, consumers have various rights under the GDPR, such as a right of access, a right to rectify incorrect information, and – where consent is the legal basis for processing personal data – a right to withdraw that consent.

But the nature of consent and how it is given is troublesome. There is a perception in the healthcare industry that consent is a means of providing patients with control over their data, but consent can be a complicated concept. Digital healthcare often involves two legal regimes coming together – traditional healthcare regulation and data protection. Consents to use patient data can involve these overlapping regimes. Under healthcare regulation, pharma companies may well require the consent of individuals in certain circumstances. For example, clinical trial sponsors must obtain the informed consent of clinical trial participants.

However, the position may not be the same under data protection laws. Under the GDPR, every processing activity requires a ground for processing. When processing a "special category of data" such as health data, an additional ground is also required. The key point to appreciate is that consent may be just one of several grounds on which companies can rely under the relevant provisions of the GDPR. Others may be available.

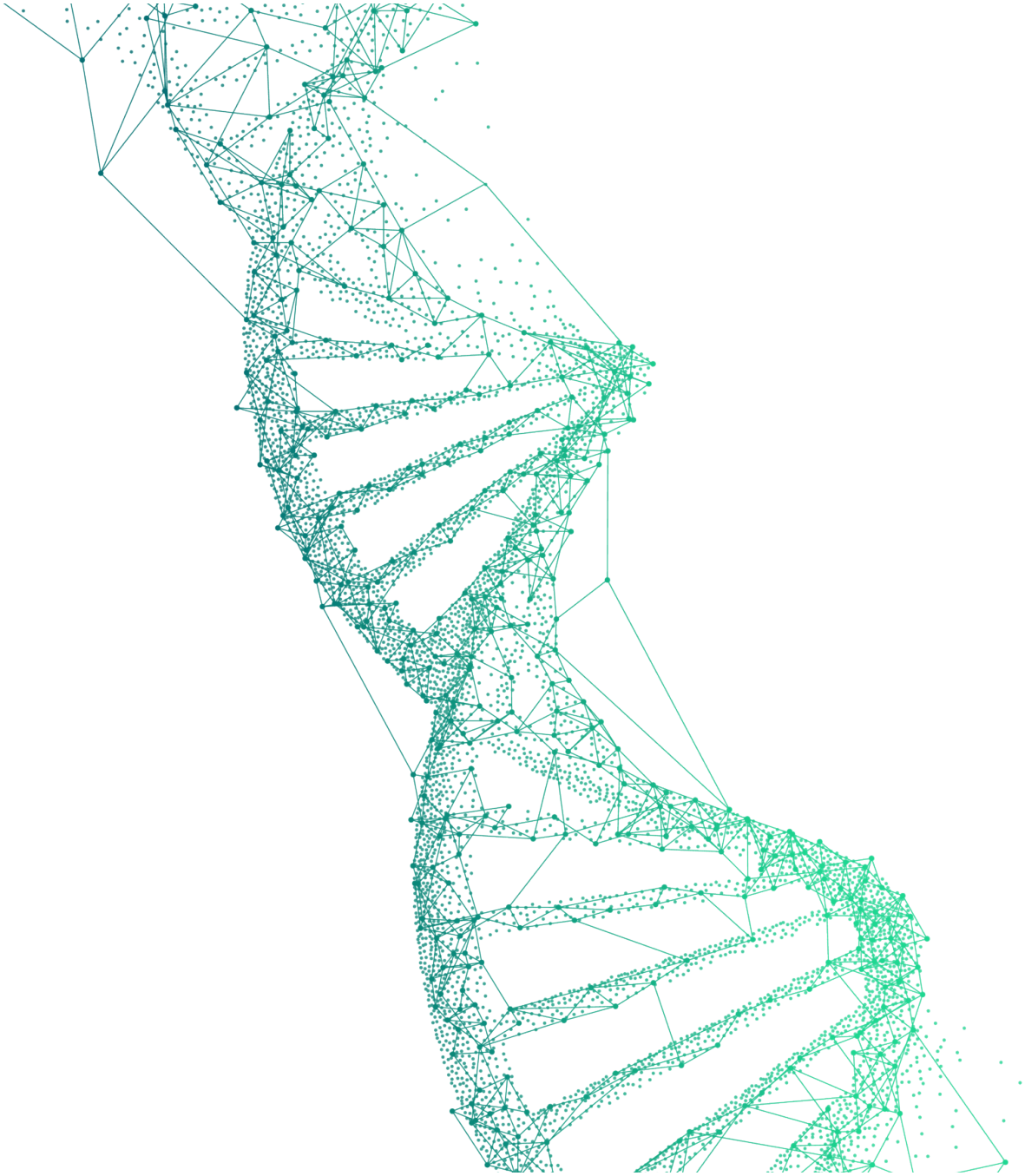
What's more, consent may not always be the most appropriate or achievable ground to legitimise data processing. Consent under the GDPR is a high bar, and must be "freely given, specific, informed" and an "unambiguous indication of the data subject's wishes". The consent required to process health data represents an even higher standard, which may be difficult to achieve in practice.

Another practical issue with GDPR consent is the right for data subjects to withdraw consent. As a general rule, if consent for a particular purpose is withdrawn, all data processing by a controller for that purpose must stop going forward. If there's no other lawful basis justifying further processing of the data, the controller must delete the relevant data.

This could be problematic when it comes to medical research, particularly if there is a small patient population. Will deleting such data diminish the utility or validity of a dataset? It may be more suitable to rely on other legal grounds, such as legitimate interests or a task in the public interest (under Article 6 of the GDPR), and public interest in the area of public health or scientific research purposes (under Article 9 of the GDPR).

Companies should note that the approach of regulators and ethics committees across Europe does vary on this issue. Whilst the UK may be gradually becoming more comfortable with a move away from GDPR consent in this context, other jurisdictions are still insisting on obtaining GDPR consent in certain contexts relating to healthcare, such as clinical trials.

The overall aim should be to ensure flexibility in use of the data, while respecting and complying with data protection laws.



Baker McKenzie.

Building trust in digital health

Understanding the five types of digital health consumer

Building trust in digital health

Our research proves that a lack of trust is a key barrier to the adoption of digital health. It is now business critical that healthtech and pharma demonstrate they are able to protect sensitive personal information, or consumers say that they will avoid new digital health technology in favour of traditional approaches.

But building trust among a disparate population is difficult. The motivations and fears of consumers in relation to digital health and data protection vary – we don't think and act as one. To help navigate these differences and build trust more effectively, here we set out the five key types of digital health consumer apparent in our survey, and their attitudes to sharing personal information.

"Traditionalist" and "Controller" groups are often most reticent to change with regard to digital health, and tend to be made up of older respondents who are 51 and older. "Controllers" in particular are less willing to share their data than any other group. "Sceptics", on the other hand, trust digital health more, but are suspicious of the commercialisation of their personal information.

At the other end of the spectrum, "Democrats" and "Innovators" are the most welcoming of new digital health products. "Democrats" in particular possess a strong desire to improve care for all, and support the use of their personal information for the collective good. Companies operating in the healthcare ecosystem will need to bear these distinctions in mind when addressing consumers' data concerns, tailoring messages to appeal to a particular target group's core concerns and motivations.

"There is an opportunity to reduce levels of reluctance to share data by providing more and better information. Such provision of information is also a huge opportunity to engage with patients around the benefits digital healthcare solutions can provide. Patient associations are already emerging as stakeholders who can play an important role in demonstrating these potential benefits. An innovative example of this is the SmartCareCF initiative led by the Cystic Fibrosis Trust."

Duncan Reid-Thomas, Partner, London

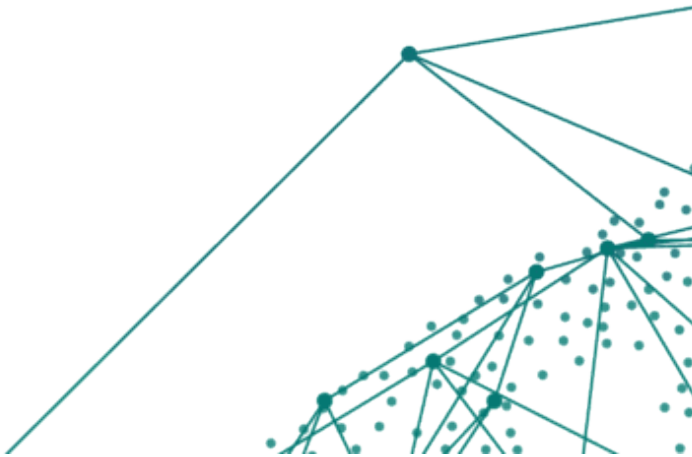
Regulating for data transparency

The GDPR is designed to increase consumer awareness about the use of their data. But our survey shows consumers desire more transparency with their data, with two thirds (65%) saying that greater transparency would build trust in digital health products.

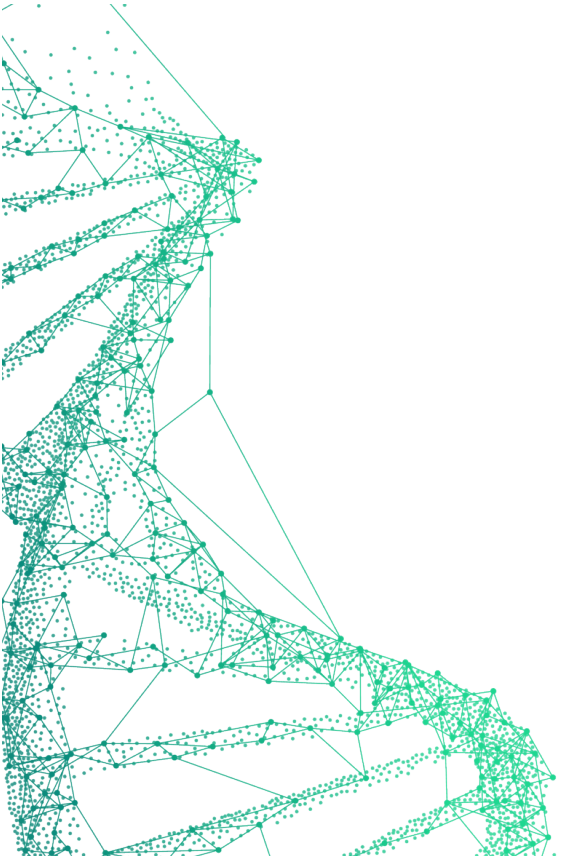
That our research highlights little consumer understanding in this area is problematic for pharma and medtech companies. Under the GDPR, controllers are required to provide intelligible and easy to understand explanations of how health data may be used in the form of data privacy notices. These privacy notices should be setting out a number of items, including:

- The identity of the data controller
- The purposes for which the data will be used and why
- Who the data will be transferred to or shared with

To allay consumer concerns, it is important that privacy notices are not seen as a tick-box exercise. Instead, when they are done well, privacy notices can form part of a data controller's overall brand strategy, and be a genuine means of reassuring consumers that a controller handles their data security concerns seriously.



The five types of digital health consumer



Traditionalists

Traditionalists are resistant to digital health products. They have a limited understanding of the potential value of digital health products to patients and a strong preference for retaining the health status quo.

Typical age: 51+
Typical health status: Chronic conditions
Typical location: Rural
Typical income bracket: Under £10k
Typical education bracket: Secondary

Key findings:

- Traditionalists have the lowest digital health adoption of any group and lowest appetite for using digital health products in future.
- They report among the lowest trust in digital health products – up to 7% below average.
- Up to 72% of respondents in this group have a preference for traditional health approaches (versus digital or a combination of both).
- As many as 8% more Traditionalists don't believe patients get the same standard of care from digital health versus traditional.

Controllers

Controllers are more receptive to digital health than Traditionalists but have significant security concerns about sharing personal information, and the strongest impulse to control the flow of their data.

Typical age: 51-64
Typical gender: Women
Typical health status: Chronic condition
Typical location: Rural
Typical income bracket: Under £10k
Typical education bracket: Secondary

Key findings:

- Controllers are far less willing to share their personal information currently and in the future.
- The security of personal information and maintaining control and ownership of this information are cited as significant risks by a disproportionately high number of consumers in this group – up to 9% more.
- 71% of Controllers don't know what personal information their medical providers hold about them – the highest of any group.
- 69% want to regain control of their data.

Sceptics

Sceptics are savvy individuals with relatively high trust in digital health, an advanced understanding of digital health and good awareness of the value of their personal information. But they also harbour the greatest suspicions about its commercialization.

Typical age: 31-40
Typical health status: Reasonable health
Typical location: Urban
Typical income bracket: £51k+
Typical education bracket: Undergraduate+

Key findings:

- Sceptics are the most open of any group to digital and combined healthcare approaches for the diagnosis and treatment of medical conditions.
- 7% more Sceptics than average say they understand how their information is used in relation to digital health.
- Over half are also willing to provide their personal information in exchange for personalized treatment – 4% greater than average.
- But they are also more wary than any other group of healthcare companies misusing their data, insurers profiting from their information or employers using their healthcare data to discriminate against them.
- Sceptics display the greatest mistrust of pharma companies – believing they have the most to gain from digital health (compared to patients or public health).

Democrats

Democrats possess a strong desire to improve care for all and support the use of their own personal information to create new digital health products for the collective good. They are the least likely to worry about exercising personal control over their data.

Typical age: 41-50
Typical health status: Non-chronic conditions
Typical income bracket: £71k+
Typical education bracket: Postgraduate / Doctorate

Key findings:

- More Democrats are willing to share their personal information in future than any other group.
- They are also more likely to rank quality of care in their top three reasons for sharing personal information to access digital health products.
- Democrats rank security, control and ownership outside the top three risks of engaging with digital health – appearing up to 9% less often than any other group.
- Democrats are particularly willing to share data if it improves the efficiency of the national healthcare system, accelerates access to healthcare nationally and to build new digital health products for the collective benefit.

Innovators

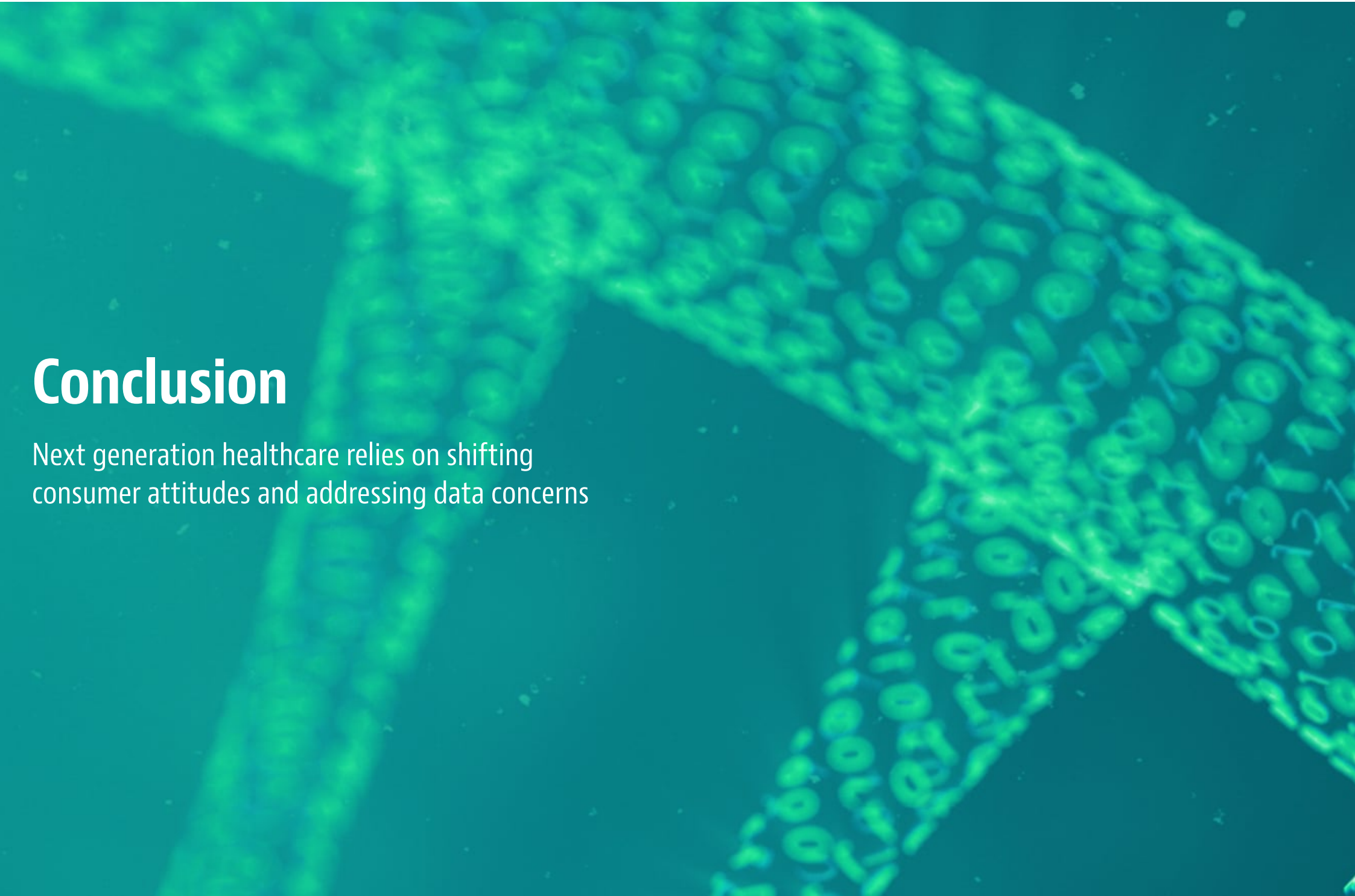
Innovators are pro-digital individuals with a positive view of digital health and higher than average risk appetite. They are already benefiting from digital health and remain keen to reap personal reward.

Typical age: 18-30
Typical gender: Men
Typical location: Urban
Typical income bracket: £31-50k
Typical education bracket: Undergraduate+

Key findings:

- 85% of Innovators have used digital health products in the past 12 months – including more complex products than any other group.
- 58% say that a shift towards digital health will improve the speed and accessibility of healthcare – 7% higher than the average.
- Concern over sharing personal information tracks consistently below average among Innovators – the perceived risk of personal information being hacked, data being used for a different purpose than stated and data being misused by a technology company are less worrying for up to 6% of Innovators.
- 55% say knowing more about the personal benefits of digital health would encourage them to use more digital health products – 10% higher than average.

Baker McKenzie.



Conclusion

Next generation healthcare relies on shifting consumer attitudes and addressing data concerns

The digital future

Digital healthcare has the capacity to improve healthcare outcomes, to increase efficiency and to open up new commercial opportunities for the public and private sectors. But many consumers remain unconvinced.

Mistrust and misunderstandings have made consumers reticent to share their data – guarding their information to exercise control at the expense of digital healthcare adoption and innovation. But it is important too, to acknowledge that data security presents a real and present fear for many consumers. Even with a strong legal regime, breaches do happen.

65%

Nearly two thirds say greater transparency would build trust in digital health products

The future of healthcare is digital. It is inevitable. But leading the market to willingly adopt new technology will be more effective than forcing the issue without consideration of individual consumer concerns and needs. If we are to shift attitudes towards digital healthcare – from concerns around security and misuse to being a key driver of healthcare transformation – pharma and medtech companies need a new approach to engaging with patients. By increasing knowledge of the protections and frameworks already in place, we can help to build trust in the next generation of healthcare.

"Digital healthcare is already transforming lives – making treatment more accessible, improving health outcomes and easing the grind on patients of managing complex conditions. It also holds the key to future breakthroughs. But without consumer trust and participation, innovation could stagnate."

Ben McLaughlin,
Chair of the Global Healthcare & Life Sciences Group, Sydney

About the research

Opinion research was conducted in Spring 2019 among 2,000 UK-based consumers. Study participants included a representative sample of men and women of differing ages, educational backgrounds, income groups and states of health.

Baker McKenzie.

Key Contacts

Helping clients overcome the challenges of competing in the global economy

Key Contacts

Ben McLaughlin
Chair of the Global Healthcare & Life Sciences Group, Sydney
Email
View bio

Hiroshi Sheraton
Partner
London
Email
View bio

Dr Isabella Liu
Partner
Hong Kong
Email
View bio

Amy de la Lama
Partner
Chicago
Email
View bio

Jane Hobson
Partner
London
Email
View bio

Duncan Reid-Thomas
Partner
London
Email
View bio

John Leadley
Partner
London
Email
View bio

Sergei Lomakin
Partner
Moscow
Email
View bio

Julia Gillert
Senior Associate
London
Email
View bio

Jaspreet Takhar
Associate
London
Email
View bio

Baker McKenzie.

Thank you for reading

Outside The Comfort Zone