beazley

Digital health at an inflection point

From growth to governance

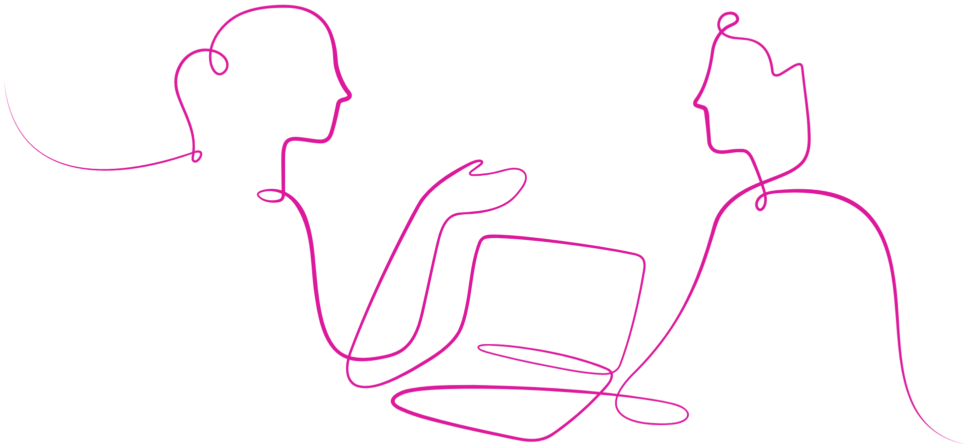
Introduction

The digital health sector has hit an inflection point. It is no longer a growth story. It is becoming an accountability story.

After years of pandemic-fuelled demand, abundant capital and technological innovation, the market is now recalibrating. Growth has cooled. Regulatory scrutiny is intensifying. AI is transforming care delivery. And risks that once sat in separate silos are converging.

What matters now is no longer simply innovation and scale. Success increasingly depends on accountability, resilience and the ability to manage interconnected risks.

Our 2026 Digital Health & Wellness survey of 600 digital health and wellness executives reveals an industry transitioning from growth to governance.



Five forces reshaping the sector

1 **Risk is more complex and interconnected**
Cyber, clinical, regulatory and technology risk increasingly overlap. A single event can trigger regulatory investigations, litigation, reputational damage and patient harm.

2 **AI is rewriting accountability**
AI adoption is accelerating across diagnosis, triage, treatment, patient support and business administrative services. As automation deepens, digital health is becoming a bellwether for how society navigates the ethical, regulatory and operational challenges of the AI age.

3 **Human and cyber risks dominate**
Executives increasingly view workforce competency and cyber threats as more significant risks than traditional clinical exposures. Cyber incidents now also have the potential to create physical patient harm.

4 **Regulation is catching up**
Privacy litigation, data-sharing disputes and regulatory ambiguity are creating increasing uncertainty for virtual care providers and digital health businesses globally.

5 **Claims are becoming more important than cost**
As claims become more complex and interconnected, digital health firms are placing greater value on claims handling for multiple coverages: medical professional and cyber liability, tech E&O, products and general liability. Insureds increasingly value long-term risk partnerships.

At a glance – the numbers that matter

58%
of executives expect their business to shrink over the next 12 months

53%
now purchase a single tailored multi-risk policy, up from 40% in 2024

77%
plan to use AI in diagnosis

81%
plan to use generative AI in treatment

32%
identify cyber risk as a leading concern

36%
identify competency and professional representation risk as a leading concern

Source: Beazley 2026 survey undertaken with 600 executives from digital health and wellness businesses based in Europe, North America and Asia.

The sector grows up

Softening growth expectations do not signal decline. They signal maturity.

Digital health as a sector is moving beyond its start-up era into a period defined by governance, accountability and resilience.

The most successful digital health and wellness organisations will be those that can navigate the growing interdependencies between technology, patient safety, data protection, regulatory compliance and reputation. As AI-enabled services and connected health ecosystems become more prevalent, organisations that balance innovation with robust governance, ethical decision-making and effective risk governance will be best placed to drive sustainable growth, improve outcomes and earn long-term trust from patients, partners and regulators.

For insurers, brokers and business leaders alike, the challenge is no longer simply facilitating growth. It is helping to build trust, resilience and confidence in one of the most important transformations in modern healthcare.

In this environment, businesses need long-term insurance partners who bring clarity, consistency and confidence to their underwriting, and efficient, prompt and dependable claims performance they can rely on.

Risk and confidence in digital care

Percentage of global executives who selected these options linked to their growth expectations, and confidence in their insurance buying in Beazley's survey undertaken in 2024 and 2026.

The accountability shift

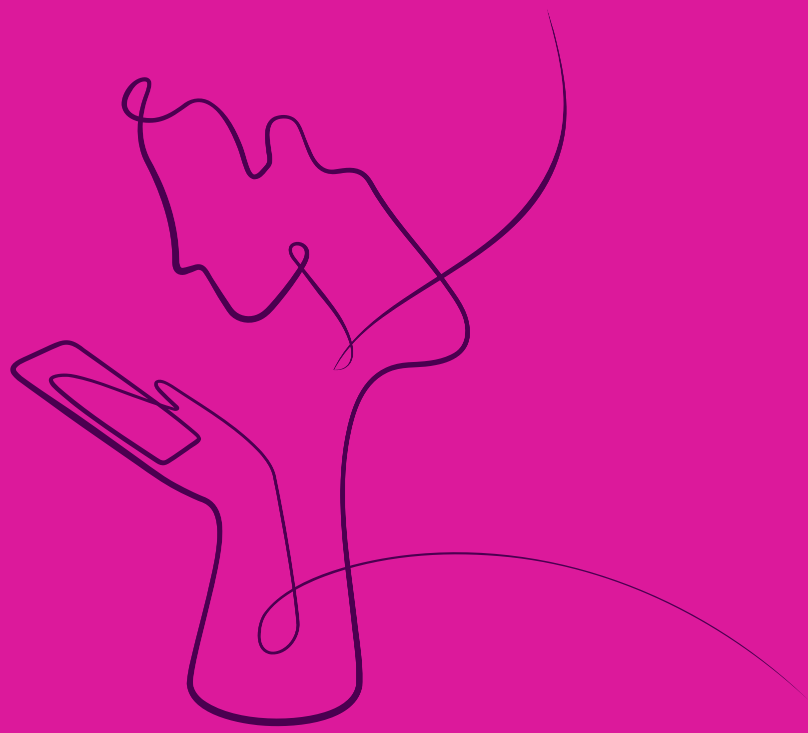
From growth-led expansion to governance-led resilience

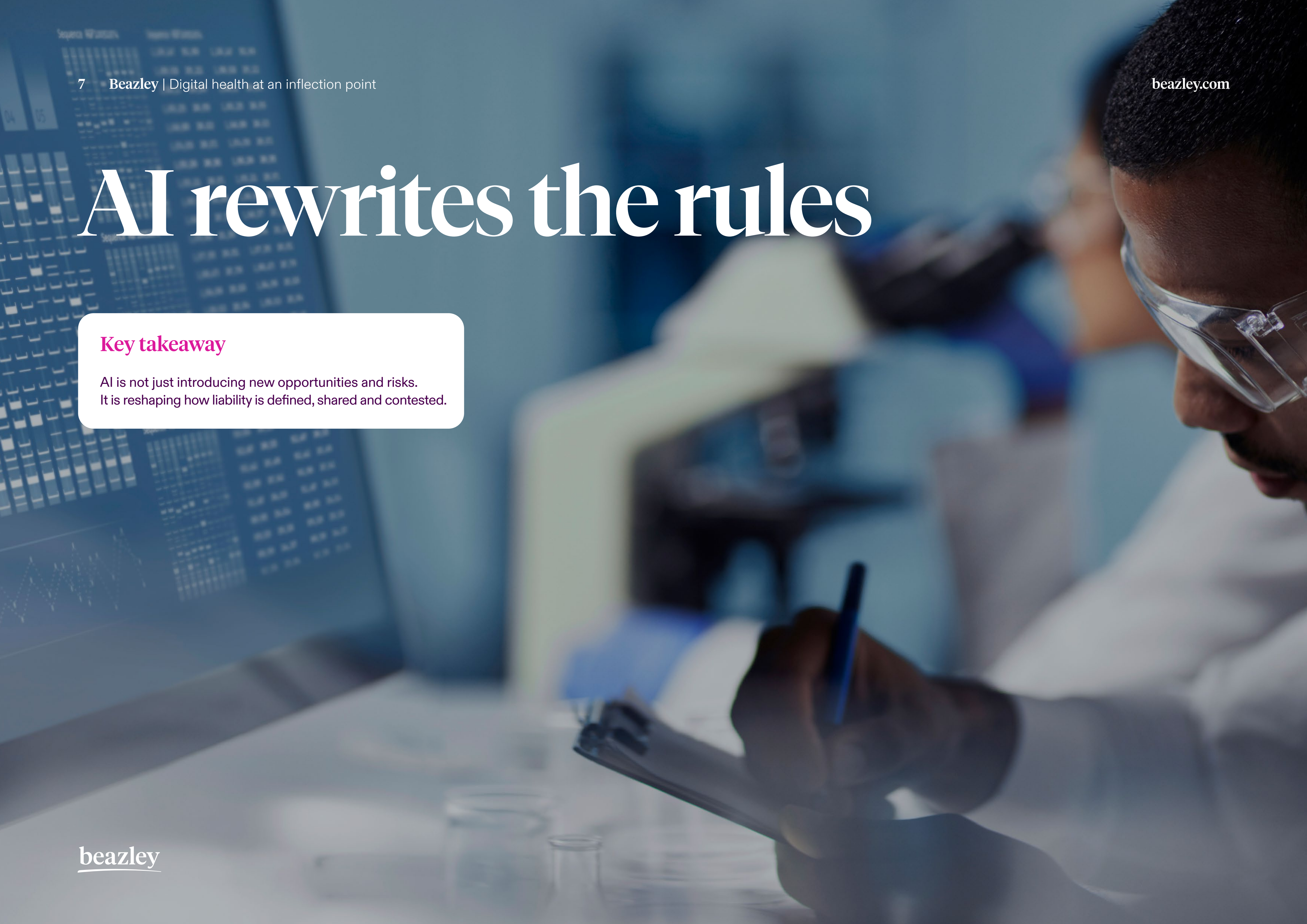
Growth →	Governance →	Liability →	Resilience
Pandemic demand	Regulation	Privacy litigation	Trust
Abundant capital	Data privacy	AI accountability	Operational maturity
Rapid expansion	AI oversight	Cyber harm	Sustainable growth
Telehealth adoption	Risk convergence	Shared liability	Long-term resilience

Digital health grows up

The digital health industry is entering a new phase. Success increasingly depends on the ability to manage interconnected regulatory, cyber, clinical and technology risks while continuing to innovate responsibly.

Index





AI rewrites the rules

Key takeaway

AI is not just introducing new opportunities and risks.
It is reshaping how liability is defined, shared and contested.

AI rewrites the rules

Digital health is emerging as the testing ground for how AI operates in high-stakes environments, where errors can directly affect patient outcomes. AI is woven through every layer of digital healthcare, powering faster diagnosis, smarter triage, and more personalised care. In addition, administrative workflows increasingly include automation across every aspect of documentation including billing, scheduling, and operations.

> “Administrative AI, including triage, intake, chatbots and portals, is already affecting claims, as patients may not realise, or consent to, the fact that they are interacting with chatbots. This complexity in how information is received and provided is making it easier for patients to allege miscommunication.”

Keri Marmorek
Claims Team Leader – Healthcare Claims, Beazley

The accountability problem

While humans are still responsible for legal oversight, AI is making accountability harder to assign, as the lines are blurred as to who or what has delivered care. This is particularly the case when it may be unclear whether patients understand how and when they are talking to a bot versus a clinician, and when the record of these interactions is unclear, for example where the algorithm fails to transfer critical information.

As treatment choices proliferate, a new, more fundamental question is emerging over how to determine what form of treatment is in the patient’s best interest.

> “Organisations are navigating a live question of whether the use or non-use of AI could affect the standard of care, potentially exposing them to liability either for not adopting new technology or for failures when using it.”

Carolyn Conners
Head of Healthcare, Beazley

Despite the emerging tension over care models and standard of care, organisations are doubling down on the increased use of AI and robotics in their operations.

What does AI look like in digital health 2026?

AI is now fully embedded in:

- Patient interaction and triage
- Diagnosis and monitoring
- Personalised treatment and care plans
- Administrative workflows

Big bets on AI and robotics in 2026

According to executives in our survey, the use of AI is set to increase over the next 12 months:

- **76%** agree they are planning to create generative AI systems for use in their business
- **81%** are planning to use or increase the use of generative AI in the treatment of patients
- **77%** are planning to use or increase the use of AI in the diagnosis of patients
- **78%** are planning to use or increase the use of robotics to create, provide or support new healthcare services
- **79%** agree that the future of healthcare is personalised services driven by greater data and tech insight

This represents a significant shift from 2024 when concern over such issues meant the focus was on bricks and mortar expansion. In fact, developing a face-to-face service dropped from 1st to 7th priority between 2024 and 2026.

Although 79% of executives express confidence in their AI risk management capabilities, confidence in managing bias and trust-related risks is growing. However, concern surrounding intellectual property (IP) protection remains consistently high since 2024.

- **74%** are concerned about bias in generative AI (78% in 2024)
- **73%** are concerned about trustworthiness of AI (80% in 2024)
- **79%** are concerned about intellectual property protection (same as 2024)

Source: Beazley's Digital Health & Wellness 2024 and 2026 surveys.

Such concerns should not be taken lightly.

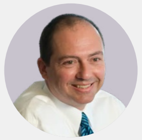
Trust is essential yet fragile in virtual care services. Patients need confidence that their data is protected and systems are reliable. Clinicians must trust AI-generated inputs enough to use them in practice. Bias is equally critical: as under-represented groups in training data can face mis-triage or misdiagnosis, create clinical safety risks and expose organisations to regulatory scrutiny.

Enabling innovation

As AI makes new approaches possible, insurance is being called upon to aid innovation.

As we look to the future, digital health companies will increasingly need to rely on experienced insurance partners with the knowledge, insight and data to risk-share with businesses.

> **"Right now, we are playing in a sandbox of AI exposures and possibilities. We are actively underwriting through emerging risks generated by the use of AI, including treatment without contemporaneous human oversight. We can take that risk and be part of this innovation journey."**



Evan Smith
Growth Leader Global Healthcare, Beazley

Best practices and risk controls

As AI becomes embedded, the insurance market is looking hard at what constitutes best practice for insureds. This includes the importance of data sourcing (focusing particularly on concern over copyrighted or sensitive information) and the role of supplemental questionnaires in identifying and managing AI-related risks.

> **"We're revising our healthcare professional services, tech and cyber coverages and developing affirmative AI coverage across our coverages. This includes explicitly addressing AI use in diagnosis, prescribing, treatment decisions and cyber and tech exposures. We have introduced a supplemental AI questionnaire and are developing AI underwriting guidelines and affirmative policy language to provide greater clarity around coverage intent and scope."**

Marc Martin
Product Leader Digital Healthcare, Beazley

The human and digital threat

Key takeaway

The industry's threats are no longer only clinical and human. They are increasingly digital too. Competency gaps and escalating cyber risk are reshaping the sector's exposure. As talent thins and cyber attacks grow more capable of causing real-world harm, digital health companies face a new era of operational and systemic vulnerability that demands stronger oversight and resilience.

The human and digital threat

Two existential risks dominate the industry – human and digital, not clinical. They centre on:

Competency

- **36%** of executives globally are concerned clients may complain that treatment, advice or exercise was not as advertised, or that professional qualifications, competence or experience were unfairly represented.

Cyber

- **32%** of executives globally worry most about cyber attack, data theft, ransomware, security breach, system failure or supply chain impact.

Source: Beazley's 2026 Digital Health & Wellness survey.

Together, they reflect a shift from traditional malpractice toward operational and systemic risk drivers.

When expertise becomes scarce

Competency remains the most acute risk at both sector and individual business level, compounded by ongoing practitioner recruitment and credentialling challenges cited as a top business risk by a further 29% of leaders.

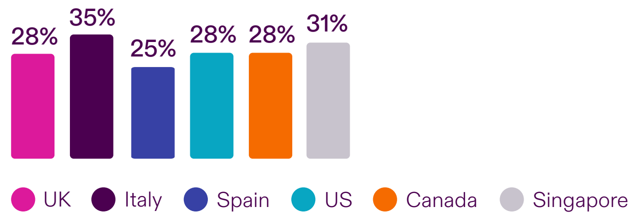
One reason why competency is such an issue is the difficulty businesses have keeping track of a digital health workforce, many of whom are independent or third-party contractors. Strikingly, three quarters (75%) of executives are troubled by lack of training or employee turnover, which makes it hard for businesses to ensure that the right people are always doing the right things.

> A lot of our clients are treating vulnerable populations. So, it's important clients know their staff and their history. It's one thing vetting people on entry, but businesses need to keep up the scrutiny as team members change. Staff might report well when they come in the door, but then something happens."
>
> **Evan Smith**

The industry is also grappling with a severe talent shortage. Few people combine the clinical, technical, commercial and regulatory skills now required. Many seasoned professionals are simply retiring, burning out, or unwilling to shoulder the rising cost of ongoing training. The sector's image isn't helping either, dampening interest among younger talent and shrinking the pipeline even further. In the meantime, pressure mounts on a scaled-back workforce to keep up with innovation and shifting demand.

Which business risk concerns you most?

Ability to recruit, retain and check credentials of practitioners



Percentage of global executives who selected this business issue as the risk that concerned them the most in Beazley's survey undertaken in 2026 with 600 executives from digital health and wellness businesses.

> Workforce shortages and recruitment challenges can lead to increased claims, especially when clinical oversight is lacking. This in turn raises concerns about the evolving standard of care as companies increasingly adopt AI and technology, making clear policies, procedures, human guardrails and oversight more important than ever."
>
> **Carolyn Conners**

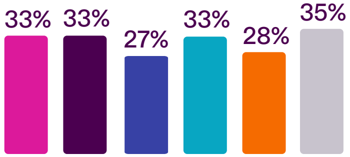
When cyber becomes clinical

Cyber risk is a systemic threat, hardwired into every digital operating model. In virtual care, it spans everything from real-time data interception via pixels and chatbots, through unauthorised disclosure of health data through marketing tools, to ransomware targeting high-value patient records, weak remote-access controls and vulnerabilities across cloud and third-party systems.

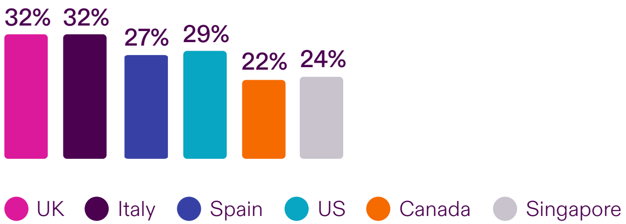
In this high-stakes environment, a single misconfiguration or marketing misstep can trigger major financial, regulatory, and reputational fallout. No wonder almost a third of executives globally cite data theft, ransomware and system failure as top risks.

Top cyber risks

Cyber attack, leading to data theft, ransomware, security breach, system failure or supply chain impact:



Cost to inform customers of a data breach and theft:



Percentage of global executives who selected these risks as the ones that concerned them the most, in Beazley's 2026 Digital Health & Wellness survey.

The threat becomes physical

Although incidents remain mercifully rare, cyber attacks have already caused actual bodily harm in healthcare. Ransomware attacks on hospitals have delayed treatments, shut down electronic health records, and forced clinicians into unsafe manual workarounds[9] Remote-monitoring platforms and connected medical devices have been disrupted by cyber incidents, interrupting insulin delivery, cardiac monitoring, and telehealth-based triage[10].

Even when attacks don't directly manipulate devices, the operational paralysis they create can lead to missed diagnoses, medication errors, and delayed emergency responses.

As virtual care becomes more dependent on cloud platforms, APIs, and continuous connectivity, the risk of cyber events translating into physical harm is no longer theoretical. It's an escalating reality.

21% of executives report they are now concerned by the potential for cyber attacks to cause physical injury.

Source: Beazley's 2026 Digital Health & Wellness survey.

Vigilance essential

Looking ahead, resilient organisations will need to prioritise removing high-risk tracking tools from patient interfaces, enforcing strict vendor and API controls, and securing remote-access pathways with strong identity management.

Continuous monitoring for ransomware and phishing threats, rigorous encryption and audit logging for all sensitive medical data, will also be essential, backed up by close oversight of marketing technologies to prevent unlawful data sharing.

> **"The most resilient organisations treat privacy and security as a single discipline, run regular risk assessments, and ensure every digital workflow, from intake bots to telehealth platforms, is designed to minimise data interception, disclosure, and third-party leakage."**
>
> **Evan Smith**

Regulatory limbo impedes innovation

Key takeaway

Multiple legal precedents have now established that digital health and wellness companies and health-adjacent apps can mishandle, intercept, share, or inadequately protect sensitive health-related data. This means coordination between marketing and legal teams, robust privacy policies and excellent incident response capabilities are essential to mitigate litigation and the related financial risks.

Regulatory limbo impedes innovation

Across all markets, businesses are navigating overlapping, ambiguous and rapidly evolving regulatory frameworks. Almost a quarter (23%) of businesses continue to cite meeting regulatory requirements as a primary operational risk for their business.

Privacy becomes a battleground

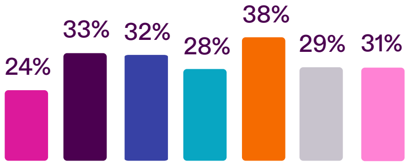
In the US, hospitals and digital health companies are navigating a patchwork of unclear, overlapping and sometimes conflicting rules. These include HIPAA (the federal Health Insurance and Portability and Accountability Act)[1], CIPA (the California Invasion of Privacy Act)[2] and CMIA (California Confidentiality of Medical Information Act)[3].

Cases brought under these laws have made clear that digital medical history bots, symptom-checkers, and online doctor–patient chat tools can be seen to constitute unlawful 'wiretapping' when they transmit patient inputs to third parties without their consent or knowledge.

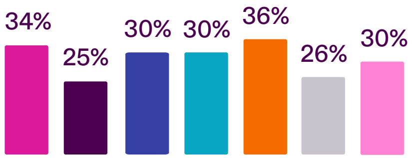
Regulatory action a global concern

Right across the regions we survey, regulatory complexity is raising compliance risk and, with it, concerns over likelihood and severity of litigation.

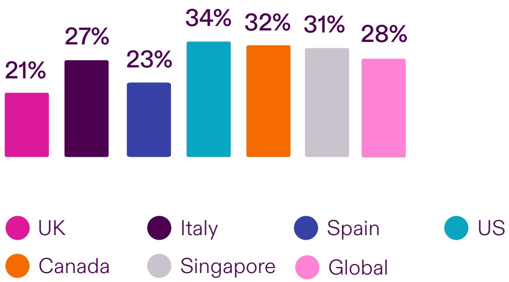
Regulatory action and associated fines



Time and cost to investigate and remediate risks



Legal action from customers or affected parties



Percentage of global executives who selected these options as their top three concerns in Beazley's survey undertaken in 2024 and 2026 with 600 executives from digital health and wellness businesses based in Europe, North America and Asia.

Marketing missteps cost millions

It is not just the way companies use technology to gather and share information for legitimate care purposes that is the issue. Marketing overreach is also coming under scrutiny.

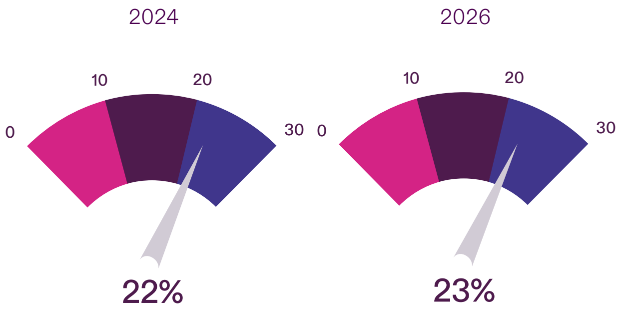
An increasing number of companies face legal action for sharing medical-related browsing behaviour. Often cases centre on companies using re-targeting pixels or SDK (software development kit)[4] trackers on symptom pages and sending sensitive user information to advertising platforms without consent.

> **"More privacy litigation is inevitable as plaintiff firms exploit ambiguity using new scanning tools to identify SDKs and tracking technologies inside apps. We see lawsuits being filed for breaches affecting as few as 90 people. Privacy litigation is no longer about scale, it's about opportunity."**

Katherine Heaton
Claims Focus Group Leader – Cyber Services & InfoSec Claims, Beazley

Regulatory risk concern over time

Meeting regulatory requirements



Percentage of global executives who selected this business issue as the risk that concerned them the most in Beazley's survey undertaken in 2024 and 2026.

As a result, regulatory actions, enforcement activity and associated fines remain the consequence of risk that worries leaders most.

Consumer expectations encourage organisational over-reach

The surge in demand for weight-loss drugs illustrates how hard it is for organisations to meet consumer demand responsibly. The frenzy of demand led to shortages of core products and pushed 503B pharmacies, manufacturers and telemedicine providers to compound their own versions[5]. The issue was not the ingredients themselves, but that many of these new formulations were not approved in this form or for this purpose.

Even after the shortages were resolved, compounded versions remained widely available, leading to increased regulatory scrutiny, with 30 telehealth businesses receiving official FDA warnings[6].

> "Risks increased for insurers and consumers when global demand for GLP-1 agonists skyrocketed, and some telemedicine start-ups turned to compounding... There are those who play by the rules, those who don't and those who push the boundary until they get sued."
>
> **Evan Smith**

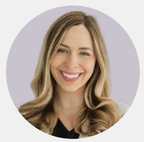
Complexity in UK, EU and Asia

Managing regulation and consumer expectations is no easier to navigate outside the US.

In the UK and Europe, companies sit at the intersection of medical device rules, AI-specific regimes (like the EU AI Act[7]), health data frameworks (including GDPR and the coming European Health Data Space[8]) and telehealth rules. There is also debate on whether an AI tool is a wellness service or a medical device, and over what constitutes valid secondary use of health data across borders.

In Asia, rapidly evolving or fragmented national rules, patchy guidance on AI in care, and data-localisation or cybersecurity laws make cross-border virtual care and cloud-based AI models hard to scale.

> "Organisations find themselves in a regulatory grey zone. They're expected to comply with requirements set by medical boards, state regulators, the FDA, and similar authorities worldwide, yet many requirements remain ambiguous and are evolving rapidly. Keeping up isn't just challenging – it's becoming increasingly complex."



Hannah Smith
Product Leader Miscellaneous Medical, Beazley

All eyes on claims as liability shifts

Key takeaway

Rising privacy litigation, cyber incidents, misinformation and emerging AI-related exposures are making disputes more complex and costly. In this environment, fast, reliable and experienced claims handling, and long-term insurance partners should be a key requirement for insurance buyers.

All eyes on claims as liability shifts

The surge in privacy litigation, cyber incidents, and regulatory scrutiny is forcing digital health leaders to shift their focus from growth to governance. Rising losses from ransomware, wiretapping claims, and regulatory interventions mean executives are spending more time on compliance, contractor and vendor oversight strategies than ever before.

In a leadership climate defined by caution and cross-functional risk awareness, where a single privacy or cyber slip can wipe out brand and financial value, scrutiny of insurance partners is rising fast, and the quality of claims handling now carries far greater weight.

The claims net is widening

A rising cadence of higher value losses underpins the new focus on claims. Looking across our claims book, we see a variety of drivers including:

- Growth in privacy and IP-related litigation
- Increased disputes driven by marketing and business practices
- Rising complexity in third-party and contractual disputes.
- Expansion of claims linked to AI-related errors, including particularly information transfer and miscommunication
- More mental health and medication claims
- Misinformation and consumer trust

The result is a claims environment that is more adversarial, harder to investigate, and significantly more expensive to resolve.

Complex claims, shared liability

Against this backdrop, businesses now see claims handling as the most important component of insurance value. In 2026, our research shows:

- Fast, reliable claims payment is now the #1 purchasing factor when choosing insurance
- Trust in claims performance has overtaken price and coverage as the most important factor driving insurance purchasing decisions

The misinformation multiplier

Social media misinformation is increasingly driving more complex third-party claims.

False or manipulated content undermines the reliability of evidence, fuels disputes over what happened and enables new forms of fraud such as deep fakes and doctored documentation. At the same time, misinformation-driven harms, from reputational damage to mental health impacts, are creating new liabilities and multi-party disputes involving platforms, practitioners and insurers.

> “Social media has made it easier for misinformation to spread. For digital health, that can influence consumer perceptions, drive claims, and attract regulatory scrutiny. Whether you love it or hate it, social media is helping define the future.”
>
> **Hannah Smith**

Plaintiff lawyers are increasingly active

In the US, concern focuses on the activities of opportunistic plaintiff lawyers, exploiting operational weaknesses for financial gain rather than focusing on actual harm to patients.

> “Privacy-related claims continue at a steady pace, often driven by legal action rather than individual injury. Some, however, stem from growing public concern, particularly around health-related information. We also see ongoing intellectual property infringement claims as companies develop their own platforms.
>
> We are also seeing an increase in litigation based on marketing promises, algorithm issues and plaintiff attorneys leveraging advertising and social media practices to make ‘profits over patients’ arguments.”
>
> **Keri Marmorek**

The liability ecosystem

Claims are no longer isolated events. They increasingly involve multiple triggers, overlapping liabilities and extended legal chains.

Loss concerns vs claims reality

How perceived risks compare with the claims that drive loss frequency and severity

High loss + high claims activity	Emerging concern and established claims activity	Potential blind spots	Watch list
Risk concern: **36%** of digital health and wellness executives worry about unfair representation – treatment, advice, qualifications and competence. **24%** of executives are concerned about inadequate care due to human error. **Claims reality:** Medical negligence is the most frequent and severe cause of loss. **Improper supervision** is the **2nd** most frequent & severe cause of loss.	**Cyber and data risk concern:** **32%** of executives are concerned about cyber incidents, ransomware, data breach and system failure. **Claims reality:** **Data privacy claims** is the **3rd** most frequent cause of loss. Claims activity is established, but the frequency of cyber claims is higher than the severity of some of the claims.	**The risks generating claims are not high on executive risk radars** **Improper supervision** (**2nd** most frequent cause of loss and severity). **Breach of contract** (**4th** most frequent cause of loss and **3rd** highest severity). **Intellectual property claims** (**4th** cause of loss by severity). **Largest gap** – misrepresentation and credential concerns.	**High concern, but limited claims** **29%** of executives are concerned about providing care to patients/clients outside of the jurisdiction that they are licensed to practice in. **23%** believe incorrect interpretation of data is a threat.
Concern around professional conduct, quality of care and treatment outcomes align with the claims that are generating the highest loss activity.	Privacy remains a key claims driver, while cyber concerns are expanding beyond data breaches to include patient harm and operational disruption.	Supervision failures and contractual disputes continue to generate significant losses despite receiving less attention among executives' stated risk concerns.	These are areas of growing regulatory concern, but they are not currently leading drivers of claims frequency or severity.

Executives worry about tomorrow's risks. Claims reflect today's realities.

Data from Beazley's 2026 Digital Health & Wellness survey of 600 executives from across organisations operating in the sector based in the US, Canada, Singapore, UK, Spain and Italy. The claims rankings are based on Beazley's healthcare-related claims from the past 10 years and ranked by cause of loss with the highest frequency and by the highest severity.

> "The risks keeping healthcare leaders awake at night are increasingly digital, yet the claims being paid today are largely driven by medical negligence and supervision failures. Looking ahead, losses are unlikely to be defined by technology alone, but by the intersection of innovation, clinical judgement and effective oversight."
>
> **Keri Marmorek**

AI liability chain concern

Perhaps the greatest emerging concern from an underwriting perspective, however, is the potential for AI to create a 'liability chain'.

> "In the event of patient injury, claims are likely to target all parties involved, including tech companies, physicians, and clients, due to the interconnected nature of AI-enabled healthcare solutions."
>
> **Marc Martin**

In light of these trends, organisations are becoming more sophisticated.

> "People are seeing the need for a breadth of coverages. They recognise exposures could come from a tech product sale, from a medical product sale, from professional liability, from the use of technology delivering healthcare services, or from a breach. That's why we offer bodily injury and property damage in our tech E&O limits, our professional limits and cyber."
>
> **Evan Smith**

Avoiding litigation

Establishing an appropriate culture is fundamental to success in managing risk and avoiding litigation.

> "A strong culture of patient safety must evolve alongside technology. If organisations wait until it's too late to focus on safety, they risk learning that lesson the hard way – in litigation rather than in practice."
>
> **Hannah Smith**

Strategies for success

Organisations can deploy several strategies to help ensure they are not put in the position of having to decide whether to settle or litigate.

Brokers/clients	Insurers and brokers
Guardrails and controls ensure data hygiene standards and guardrails are enforced – with a particular focus on data sourcing and governance.	**Work to add affirmative language** within the definition of tech products, professional liability (PL), cyber and media liability products.
Support a culture that fosters unity of purpose and a sense of collective responsibility between platform, providers and professionals to improve risk management.	**Prepare AI guidelines** and a supplemental questionnaire to better assess and underwrite AI risks, particularly for health tech companies.
Carefully select counsel who understand technology, medicine and local nuances, as well as the corporate structure of virtual care companies. Recognise you may need to flex the team.	**Encourage tripartite collaboration** between insurer, broker and client to share information, maintain learning and fuel adaptation.
Hold a pre-bind meeting with claims teams to understand who will handle cases and ensure alignment on expectations and strategy.	**Become a strategic risk partner** by providing risk intelligence and educating teams on preventing the operational and cyber issues that drive today's claims.

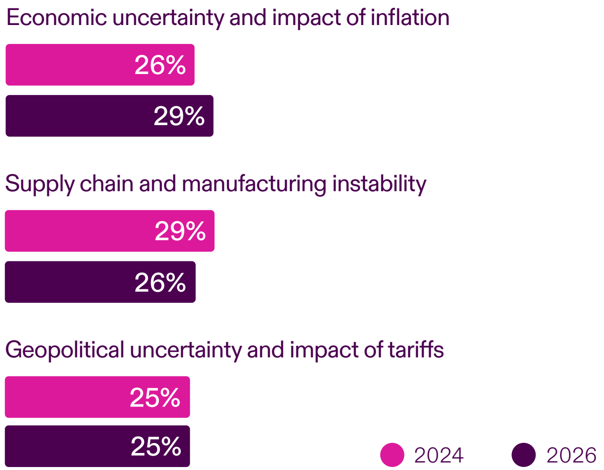
Headwinds shape strategy

Key takeaway

In tough economic conditions, virtual care success is no longer defined by growth or rapid innovation alone. What stakeholders value most today is operational resilience. In other words, a proven ability to manage complex, interconnected risks while consistently meeting the expectations of investors, regulators and patients over time.

Headwinds shape strategy

Macroeconomic, geopolitical and regulatory risks continue to dominate executives' thinking.



Percentage of business leaders who selected these options in Beazley's survey undertaken in 2024 and 2026.

What are businesses seeing?

Continually rising prices for components, energy and global transport are making devices such as sensors, wearables, diagnostics, and remote-monitoring equipment more expensive to produce and procure. Simultaneously, fragile supply chains, especially for specialised medical components, are causing delays, shortages and higher inventory costs.

Against this backdrop, it is perhaps not surprising that for the first time in our research, over half of the executives surveyed (58%) expect their businesses to shrink in the next 12 months.

> **"Ongoing economic uncertainty, inflation, and supply chain disruptions are significant operational risks for digital health businesses, affecting costs, procurement, and market strategies."**
>
> **Carolyn Conners**

In the early days of digital health during and immediately after COVID-19 in 2020–2021, major central banks pushed interest rates to historic lows, often close to zero, as part of emergency monetary support[11]. But in 2025, by contrast, inflation stood at 3.6% globally[12]. Raised inflation levels and higher interest rates place a burden on even the fastest-growing virtual care businesses. Many carry heavy debt loads and must keep hitting financial targets to maintain covenants with lenders – be that traditional banks or venture capital providers.

> **"Many telemedicine organisations borrowed a lot of money and interest rates have not been supportive. Some of the economic stress is coming from that and the debt burdens that some of these larger companies have. Many are still not making money."**
>
> **Evan Smith**

Uncertainty, instability and inflation

These macroeconomic pressures are more than external challenges. They directly increase risk exposure.
Cost pressures, supply chain disruption and operational strain heighten the likelihood of errors, compliance failures and disputes. As a result, financial and management stress is becoming a major driver of claims, particularly for smaller and growing businesses, highly leveraged firms, and organisations that fail to adapt to changing conditions.

Double whammy hits smallest hardest

Inflation, rising costs and supply-side disruption are creating a double whammy for digital health businesses. As discretionary demand weakens and operating costs rise, 33% of the small businesses we surveyed now rank economic uncertainty as their top business risk.[13] Small and mid-sized firms are feeling the strain most acutely, particularly hardware-dependent companies such as remote monitoring, diagnostics and wearables providers.

Outcomes are polarised

In this tough and unpredictable operating environment, pressure has not affected every business in the same way.

> **"Over the last five years, those who developed niches are doing well; those that tried to be everything to everyone, spent too much money and grew fast, are hurting now."**
>
> **Evan Smith**

Pushing the boundaries

Key takeaway

In a climate where governance is as important as growth, and economic uncertainty continues to challenge investment decisions, organisations are prioritising markets that offer a strong strategic fit and sustainable returns.

Pushing the boundaries

Business leaders remain clear-sighted about opportunities in overseas markets and have a continued appetite for geographic expansion. While it's still the case that most continue to favour growth in their own or existing markets, 2026 sees various new patterns emerging:

- There is a marked uptick in interest in the UK market, from both US and Canadian digital health businesses
- Asia is attracting more attention, not just from local Singaporean businesses but also from Spain
- Countries in Europe, including the UK, are showing increased appetite for broader market diversification

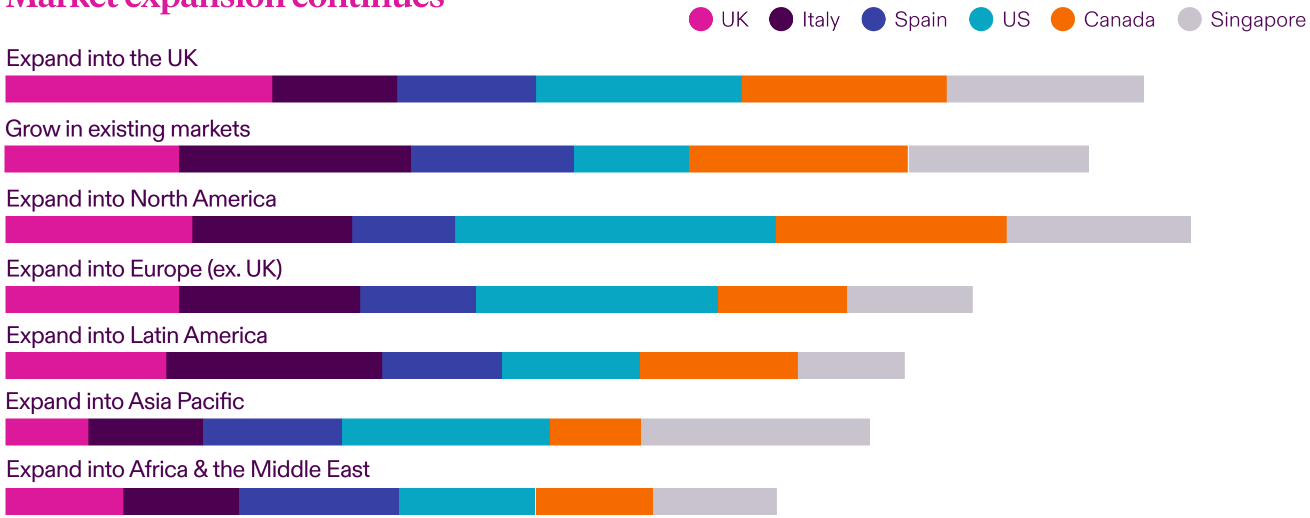
Why do North American businesses favour the UK?

The UK has become one of the most attractive, structured, and scalable markets for digital health globally, especially for firms seeking predictable reimbursement, strong institutional partners, and rapid adoption pathways. The NHS is a single, centralised buyer, with huge scale, there is active investment in digital transformation through modernisation of patient records (EPRs) and AI integration – plus the market is mature, receptive and high-yield.

Why is Asia gaining ground?

Asia is good for digital health businesses because it offers huge population scale, rapid digital adoption, strong government funding, and a high need for remote and AI-enabled care. The population is ageing, governments are investing and markets are receptive to foreign innovation. These are all conditions that favour international entrants with mature products, despite regulatory complexity.

Market expansion continues



Percentage of digital health and wellness executives that selected these market expansion options in Beazley's 2026 survey.

What drives investment into Europe?

Businesses in Italy and Spain see growth opportunities everywhere, helped by EU-wide moves from local pilots to pan-European digital health infrastructure. Interoperability reforms, AI adoption, new cross-border data frameworks and a fast-growing innovation network linking major cities and health systems are giving companies shared access to hospitals, payers and validation centres that can test and scale technologies across Europe[14].

M&A appetite cooling

Fewer than a fifth (18%) of digital health businesses globally are prioritising M&A (mergers and acquisitions) in the next 12 months as a route to expansion, likely reflecting economic and geopolitical risk rather than lack of strategic intent.

By 2030, digital health and wellness is expected to become increasingly personalised, proactive and connected, powered by AI, data analytics, wearable technologies and remote care[15]. However, achieving this vision will require:

- Scalable, interoperable and user-centric technology
- Stronger partnerships across healthcare and wellness ecosystems
- Investment focused on high-impact, outcome-driven innovation
- Robust governance, cybersecurity and risk management
- Greater emphasis on regulatory compliance and evidence-based outcomes
- Improved accessibility and health equity

Ultimately, success will depend not only on innovation, but on organisations' ability to build trust, demonstrate value and scale sustainably.

Appendix

Methodology – 2026 Survey

This report is based on a survey of 600 business leaders in the digital health and wellness sector across the US, Canada, UK, Singapore, Italy and Spain. Research was conducted by Opinion Matters on behalf of Beazley between 9–17 March 2026.

Respondents represented a range of digital health subsectors, including:

- Health and wellness practitioners
- Software and platform providers
- Health technology and life sciences technology companies
- mHealth providers
- Telehealth and telemedicine providers

The sample included an equal spread of organisations across revenue bands, ranging from US/CAN/SG$/£/€250,000 to more than US/CAN/SG$/£/€1 billion.

Previous waves

Comparable research was conducted in 2020, 2022 and 2024.

Research standards

Opinion Matters is a member of the Market Research Society (MRS) and the British Polling Council and conducts research in accordance with the MRS Code of Conduct and ESOMAR principles.

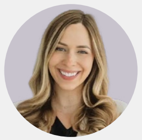
Contributors

Carolyn Conners
Head of Healthcare, Beazley

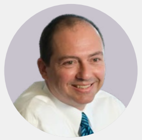
Katherine Heaton
Claims Focus Group Leader – Cyber Services & InfoSec Claims
Beazley

Keri Marmorek
Claims Team Leader – Healthcare Claims
Beazley

Marc Martin
Product Leader Digital Healthcare
Beazley



Hannah Smith
Product Leader Miscellaneous Medical
Beazley



Evan Smith
Growth Leader Global Healthcare
Beazley

References

1. Health Information Privacy | HHS.gov
2. Codes Display Text
3. https://www.accountablehq.com/post/what-hipaa-laws-protect-vs-state-privacy-laws-cmia-hb300-cpra-2025-guide?
4. What Is an SDK? Software Development Kits Explained | Okta
5. Global Rise of Compounded Weight-Loss Medicines: A Worrisome Trend - PMC
6. https://www.fda.gov/news-events/press-announcements/fda-warns-30-telehealth-companies-against-illegal-marketing-compounded-glp-1s
7. Artificial Intelligence Act EU Official Text - AI Act
8. European Health Data Space Regulation (EHDS) - Public Health
9. Ransomware's Hidden Toll on UK Hospitals – MedTechNews
10. Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication | FDA
11. How COVID-19 Has Impacted Changing Global Interest Rates | GEP Blog
12. IMF Data Brief: World and Regional Inflation
13. Revenue between US$/CAN$/SG$/GBP/EUR 250,000 and US$/CAN$/SG$/GBP/EUR 1m
14. Three Leading Digital Health Hubs Join Forces to Build a Pan-European Innovation Network | Future of Health Grant
15. Technology shifts: Delivering the Life Sciences and Healthcare 2030 predictions | Deloitte UK

beazley

Discover more
beazley.com

Beazley plc (BEZ.L), is the parent company of specialist insurance businesses with operations in Europe, North America, Latin America, Bermuda and Asia. Beazley manages six Lloyd's syndicates and, in 2025, underwrote gross premiums worldwide of $6,100.7million. All Lloyd's syndicates are rated A+ by A.M. Best.

Beazley's underwriters in the United States focus on writing a range of specialist insurance products. In the admitted market, coverage is provided by Beazley Insurance Company, Inc., an A.M. Best A rated carrier licensed in all 50 states and its subsidiary, Beazley America Insurance Company, Inc. In the surplus lines market, coverage is provided by Beazley Excess and Surplus Insurance, Inc.

Beazley's European insurance company, Beazley Insurance dac, is regulated by the Central Bank of Ireland and is A rated by A.M. Best and A+ by Fitch.

Beazley's Bermuda entity, Beazley Bermuda Insurance Limited, is A rated by A.M. Best and regulated by the Bermuda Monetary Authority.

Beazley is a market leader in many of its chosen lines, which include Directors & Officers, Financial Lines, Cyber, Property, Marine and Aviation, Reinsurance, Accident and Life, and Political Risks and Contingency business.

For more information, please go to: www.beazley.com

BZSL 505

beazley

Insurance. Just different.