

IGNITE 2026

Health Innovation Summit

From innovation ambition to system readiness:
What health leaders need to do now.

Foreword

London has long been one of the world's great centres of science, medicine, education and civic innovation. Few places bring together such depth of research excellence, clinical expertise, entrepreneurial energy, investment potential and population diversity. This concentration of capability creates a distinctive opportunity for health innovation, but it also brings a responsibility. Innovation districts do not succeed through proximity alone. They require deliberate coordination, shared purpose and the ability to connect discovery with the needs of the health system and the communities it serves. UCL has a central role to play as an anchor institution in London's innovation ecosystem. Its breadth across science, engineering, medicine, population health, social science and policy creates the conditions for new ideas to emerge and for complex challenges to be approached from multiple perspectives. UCLPartners brings a complementary and essential role as an internationally leading health innovation company, working with leading experts to invent the future of healthcare and support the adoption of innovation into practice. Together, these institutions sit at the intersection of research, care delivery, public value and place.

The IGNITE Health Innovation Summit series were designed to make that intersection productive. They bring together world experts to address provocative questions on complex challenges, and to accelerate evidence based, equitable health innovation. They provide a platform where scientific possibility can be tested against clinical reality, system pressure, public trust, workforce capability and the practical demands of implementation. The discussions at IGNITE Health Innovation Summit 2026 made clear that place-based innovation must be anchored in real clinical and operational needs. Artificial intelligence, advanced data infrastructure, cybersecurity and quantum technologies all offer significant promise. However, their value will depend on whether they are shaped by the realities of care, tested with the people who will use them, governed responsibly and adopted in ways that support staff rather than add burden.

The workforce is central to this agenda. Clinicians, care professionals, operational teams, researchers, data scientists and innovators must be equipped to use new technologies and, just as importantly, to shape, challenge and improve them. Health innovation will succeed only if it strengthens the judgement, confidence and capacity of the people delivering care.

This report sets out the leadership challenge that follows. London has the assets, partnerships and ambition to lead the next phase of health innovation. The task now is to bring them together with greater purpose, so that invention is aligned with need, institutions work across boundaries, the workforce is supported, public trust is strengthened and emerging technologies can deliver lasting benefit for patients and communities.

Dr Chris Laing, UCLPartners CEO

Acknowledgements

The IGNITE Health Innovation Summit Series brings together national and international leaders across the ecosystem to debate, connect and accelerate meaningful change. The latest Summit, held in January 2026, was co-developed by UCLPartners and UCL, blending academic excellence with on-the-ground expertise in healthcare delivery and innovation. We are grateful to all panel members and colleagues in attendance for generously sharing their time, insight and expertise, without which this report would not have been possible.

With particular thanks to:

IGNITE Advisory Committee:

Professor Alan Thompson	UCL
Professor Kevin Fong OBE	UCLPartners
Felipe Fouto	UCL
Ilias Zapantis	UCLPartners
Nasema Uddin	UCL
Mandy Trinh	UCLPartners
Professor Laura Shallcross	UCL
Professor Rebecca Shipley OBE	UCLPartners
Professor Neil Sebire	UCL
Professor Parashkev Nachev	UCL

Keynote speaker:

Caroline Clarke DBE	NHS England (London)
---------------------	----------------------

Clinical intelligence panel members:

Professor Mihaela van der Schaar (debate lead)	University of Cambridge
Professor Parashkev Nachev	UCL
Professor Folkert Asselbergs	UCL
Dr Jorge Cardoso	King’s College London

Data, governance and cybersecurity panel members:

Peter Munford (debate lead)	Vantix Partners
Dr Steve Harris	University College London Hospital
Hilary Fanning MBE	NHS England

Quantum technologies in healthcare

panel members:

Professor John Morton (debate lead)	UCL and Q-BioMed
Professor Quentin Pankhurst	UCL and Q-BioMed
Eve Worrell	Department of Health & Social Care
Faiyaz Amin	Department for Science, Innovation & Technology
Ben Hunt	Siloton

Participants

Chris Laing	UCLPartners
John Craig	UCLPartners
Kate Petts	UCLPartners
Katie Harrison	UCLPartners
Lucy Brock	UCLPartners
Kate Langford	UCLPartners
Philippa Tucker	UCLPartners
Kelly Lin	UCLPartners
Jay Stone	Nuffield Council on Bioethics
Martin Davies	Nuffield Council on Bioethics
Alex Lawrence	The Health Foundation
Lydia Ragoonanan	The Health Foundation
Tom Hardie	The Health Foundation
Surbhi Gupta	NHS England
Chris Streather	NHS England (London)
James Friend	NHS England (London)
Dominic Jones	NHS England
Geraint Thomas	UCL
Jane Kinghorn	UCL
Mani Hussain	CQC
Ambra Caruso	Health Innovation Network South London
Tim Andrews	Orcha Health
Avi Mehra	IBM
Sigal Hachlili	Guy's and St Thomas' NHS Foundation Trust
Adam Callan-Sidat	Q-BioMed
Jeffry Hogg	University of Birmingham
Amidullah Shadmaan	University of Birmingham
Matthew Jones	Innovate UK
Shani Shamah	Patient Representative
Curie Freeborn	Patient Representative

Disclosure

This report was synthesised and produced with the assistance of generative AI under human direction, with the final review and assurance of the authors, who accept ownership and responsibility for the contents of the report.

Authors: Ilias Zapantis, UCLPartners and Mandy Trinh, UCLPartners

How this report should be read

If you only have 30 minutes, we recommend reading the Executive Summary, the system readiness test and “what leaders need to do now” for each section. These sections distil the core insights from the Summit and are designed to stand alone for readers short on time. This report is a synthesis of discussions held during the Summit, not a verbatim record. In line with the Chatham House Rule, comments are not attributed to individuals or organisations.

The content reflects the themes, tensions and ideas that emerged from the room on the day, shaped by the particular mix of voices present. It is intended to prompt reflection and discussion, rather than serve as a comprehensive or definitive account of any single topic covered.



Table of Contents

From innovation ambition to system readiness: what health leaders need to do now.			
Foreword	01		
Acknowledgements	02		
Disclosure	04		
How this report should be read	04		
Executive summary	06		
Executive insights	07		
1. System readiness is needed to connect ambition to impact			
2. Clinical intelligence must improve decisions, not simply generate more insight			
3. Trusted data use is an operating condition for innovation			
4. Cyber resilience and AI accountability are patient safety issues			
5. Horizon readiness must start before technologies mature			
Executive priorities	10		
Introduction	13		
The system readiness test	15		
1. Clinical intelligence must be built around decisions	17		
Better decisions, not more predictions			
Designing decision-ready pathways for the realities of care			
Digital twins and agentic AI as decision augmentation			
Accountability for AI enabled decisions			
Workforce co-creation as a safety, usability and adoption requirement			
What leaders need to do now			
2. Data governance must enable trust, learning and system resilience		25	
Governance must enable responsible data use			
A learning health system needs minimum sufficient data			
Public trust is an operating condition for data enabled healthcare			
Cyber resilience is a patient safety priority			
Practical assurance, not performative compliance			
What leaders need to do now			
3. Quantum technologies in healthcare require strategic preparation		34	
Quantum is a strategic horizon for health and care			
Quantum sensing offers the nearer term opportunity			
Quantum computing is a longer term strategic horizon			
Post-quantum cybersecurity is an immediate leadership issue			
What leaders need to know			
Conclusion		44	

Executive summary

The IGNITE Health Innovation Summit 2026 explored “The Future of Health and Emerging Health Innovation” at a time of rising demand, workforce pressure, widening inequalities and growing digital dependency. Discussions focused on artificial intelligence, clinical intelligence, data governance, cybersecurity and quantum technologies. Across these areas, one message was clear: health innovation is moving from a question of technological possibility to a question of system readiness.

System readiness is the ability of a health and care system to absorb innovation safely, govern it responsibly, embed it into real pathways, support the workforce to use it well, maintain public trust and scale what works. It is the bridge between technological possibility and measurable benefit for patients, staff and the wider system.

This report argues that senior leaders must move beyond innovation ambition, isolated tools and short-term pilots. The task is not simply to accumulate more technologies, but to build the conditions that allow innovation to create trusted, practical and sustainable value. Three leadership priorities stand out. Clinical intelligence must improve the decisions that shape care, not simply generate more predictions, alerts or dashboards. Trusted data use, practical governance and cyber resilience must become core capabilities for a learning health system. Emerging innovation horizons, including quantum technologies, require preparation now through clinical pull, test environments, adoption routes and post quantum security planning.

The report introduces a system readiness test to help leaders assess whether innovation is responding to a real need, improving decisions and outcomes, and creating value in practice. It also helps system leaders consider whether accountability is clear, whether the workforce and workflows are ready, and whether future technology horizons are being anticipated. The next phase of health innovation will be defined not only by the potential of new tools, but by the readiness of health systems to turn innovation into sustained impact for all.



Executive insights

1. System readiness is needed to connect ambition to impact

Health systems have no shortage of innovation ambition. The harder task is building the readiness to absorb, govern, implement and scale innovation in ways that improve care. Emerging technologies will create value only when they are connected to real clinical, operational, population or infrastructure needs, embedded into pathways, supported by the workforce and evaluated in practice.

For system leaders, this means treating innovation readiness as a core leadership responsibility. Digital, research and transformation teams can support this agenda, but they cannot own it alone. Boards and senior leaders need to be accountable for whether the system is ready to use innovation safely, responsibly and at scale.

2. Clinical intelligence must improve decisions, not simply generate more insight

Improved clinical intelligence capabilities such as AI, analytics, digital twins and agentic systems will not transform care by producing more predictions, alerts or dashboards. Their value will depend on whether they improve the quality, timeliness, consistency and equity of decisions. In a pressured system with constant urgent and competing alerts, the most important element is whether clinical intelligence helps teams decide when to act, when to monitor, when to escalate, when to de-escalate and when not to intervene.

System leaders should therefore focus on decision-ready pathways.

Every priority use case should be clear about the decision being supported, who acts on the insight, what intervention follows, how uncertainty is managed and what outcome should improve and how. Without this clarity, technologies may add further noise, burden and complexity without changing care.

3. Trusted data use is an operating condition for innovation

Data governance is no longer a narrow compliance function. It is a strategic capability that determines whether health systems can learn, improve, coordinate care, support research and maintain public confidence. A learning health system needs data to be used responsibly, transparently and purposefully, with safeguards that protect patients while enabling public benefit.

The leadership task is to move away from data minimisation towards minimum sufficient data, defining what data are needed to support care, research, planning, improvement and population health. Leaders must also recognise that public legitimacy cannot be assumed. Trust must be designed into the operating model through clear explanations, visible safeguards, sustained public dialogue and evidence that data use improves care and reduces inequalities.

4. Cyber resilience and AI accountability are patient safety issues

As care becomes more digitally dependent, cyber resilience must be treated as part of care delivery. When digital systems fail, access to records, diagnostics, prescribing, communication and operational coordination can be disrupted. Cyber risk is therefore not only a technical or compliance concern, but also a patient safety and service continuity risk.

The same applies to AI-enabled decisions. As AI becomes more embedded in clinical intelligence, accountability must be clear before tools are scaled. Leaders need assurance on validation, audit, bias monitoring, escalation, supplier responsibilities and post deployment surveillance. Technical performance is the easier bar to clear.

The harder one is whether the system can govern how the tool influences decisions and learn from the outcomes.



5. Horizon readiness must start before technologies mature

Quantum technologies show why readiness cannot wait until innovation is ready for routine adoption. Quantum sensing creates nearer term opportunities in diagnostics and monitoring. Quantum computing can support biomedical discovery over time, while post-quantum cybersecurity is already a strategic issue since sensitive clinical, genomic and research data need to remain secure for decades.

For system leaders, the implication is clear. Horizon readiness means creating clinical pull early, scanning for future capabilities and risks, building partnerships, developing test environments and preparing adoption routes before technologies arrive fully formed. Without this preparation, emerging technologies risk being shaped by technical possibility rather than true health system need.

Together, these insights point to a single conclusion. The next phase of health innovation will be defined by both the technological novelty of these tools, as well as by the readiness of health systems to shape those tools around real needs, embed them into practice and turn innovation potential into measurable benefit.



Executive Priorities

The leadership task, therefore, is to move from innovation ambition to system readiness. This requires executive accountability. Boards and senior leadership teams should treat system readiness as a core responsibility, not as a delegated digital, innovation or research function. This different perspective interrogates which technologies should be adopted, and whether the system has the conditions to realise the expected benefits.

The priorities below set out what leaders should do within three time horizons, within 6 months, within 12 months and beyond 12 months, to strengthen system readiness across clinical intelligence, trusted data use, cyber resilience, workforce capability, implementation infrastructure, AI accountability and quantum preparedness.

System readiness key priorities

Executive Priority	Within 6 months Diagnose	Within 12 months build readiness conditions	Beyond 12 months Embed and scale
Start with the decisions and problems that matter most	Identify where poor, delayed or inconsistent decisions create harm, waste, inequity or avoidable demand. Create mechanisms for frontline teams to signal the problems that most need solving.	Prioritise AI, analytics and digital solutions where better decisions would improve outcomes, patient flow, prevention or equity.	Demonstrate that priority innovations are improving outcomes, equity, prevention or flow, and redirect effort where value is not being realised.
Apply the system readiness test before wider adoption	Review current innovation programmes against the system readiness test to identify what should proceed, what needs strengthening and what should stop.	Embed the system readiness framework into strategic planning, investment decisions, innovation portfolios and board assurance.	Use the readiness test as a continuing leadership discipline for adoption, scaling, redesign and decommissioning decisions, based on evidence of value.
Build trusted data use and public legitimacy	Identify where fragmented governance, unclear data sharing or low public trust is limiting care, research, improvement or population health.	Define a minimum sufficient data framework, simplify cross organisational data sharing, and create public facing explanations of how data are used, safeguarded and linked to public benefit.	Sustain trusted data use through ongoing public dialogue, transparent safeguards and evidence that data enabled innovation is improving outcomes and reducing inequalities.

Executive Priority

Within 6 months Diagnose

Within 12 months build readiness conditions

Beyond 12 months Embed and scale

Build workforce and accountability readiness

Identify where new technologies could add burden, disrupt workflow or weaken professional confidence.

Establish clear executive, clinical and supplier accountability for AI enabled decisions before wider scale.

Develop workforce capability plans for AI, data and digital care, including digital literacy, clinical and technical collaboration, and roles that bridge analytics, operations and implementation.

Co-create decision support tools with clinical, operational, technical, patient and public perspectives.

Maintain workforce confidence, usability and experience as core measures of innovation success.

Establish post deployment monitoring for AI supported decisions, including validation, audit, bias monitoring, escalation and outcomes review.

Treat cyber resilience and future data security as care delivery risks

Review cyber downtime and recovery arrangements as patient safety and service continuity risks.

Map sensitive datasets exposed to long-term security, privacy or quantum related risks, including clinical, genomic and research data.

Run cyber downtime and recovery exercises with frontline teams, linked to clinical risk, emergency preparedness and business continuity planning.

Begin post quantum security planning for long-lived sensitive data.

Maintain cyber resilience as a standing board assurance priority, with assurance that tests operational resilience, not only compliance.

Strengthen the route from discovery to adoption and scale

Identify the gaps between clinical need, innovation activity, evaluation, procurement and adoption.

Create clearer routes for emerging technologies that connect clinical need and system priorities to real world testing, evidence generation and implementation.

Prioritise emerging technology use cases that respond to clear clinical, research or infrastructure needs.

Build and embed a system wide implementation route for testing, evaluation, procurement, adoption and scaling.

Publish, maintain and act on an emerging technology readiness roadmap covering quantum sensing, quantum computing and post quantum cybersecurity.

Within 6 months: Diagnose exposure and establish ownership

Senior leaders should establish where the system is most exposed and where innovation could create the greatest value. This means identifying the problems and decisions that matter most, reviewing current AI, data, cyber and emerging technology programmes against the system readiness test, and confirming that accountability is clear before wider adoption. Boards should also review cyber downtime and recovery as patient safety and service continuity risks, and begin mapping sensitive clinical, genomic and research datasets exposed to long-term security, privacy or quantum related risks.

Within 12 months: Build readiness conditions for trusted implementation

Leaders should move from readiness assessment to readiness building. This means embedding the system readiness framework into strategic planning, investment decisions and board assurance, strengthening trusted data use, developing a minimum sufficient data approach and simplifying responsible cross organisational data sharing. Public facing explanations should make clear how data are used, why this matters, what safeguards are in place and how public benefit is delivered. Workforce capability plans should be in place for AI, data and digital care, supported by co-designed decision support tools, practical cyber resilience exercises and clearer routes for testing, evaluating and implementing emerging technologies.

Beyond 12 months: Embed, scale, monitor and sustain readiness

System readiness should become a permanent leadership capability. Health systems should build shared routes for testing, evaluation, procurement, adoption and scaling, with mechanisms to accelerate innovations that demonstrate value and stop or redesign those that do not. AI supported decisions should be subject to post deployment monitoring, including validation, audit, bias monitoring, escalation and outcomes review. Leaders should continue to strengthen workforce confidence, public trust and cyber resilience, while maintaining an emerging technologies readiness roadmap covering quantum sensing, quantum computing and post quantum cybersecurity.

These priorities are not a good practice checklist. They are the minimum conditions for responsible innovation. Senior leaders should be accountable for whether their systems can define the right problems, improve decisions, use data responsibly, support staff, maintain public trust, withstand disruption and scale what works.

Introduction

The NHS 10 Year Health Plan sets out a clear direction for the future of health and care: moving more care from hospitals into communities, shifting from analogue to digital systems, and reorienting services from treatment to prevention. These priorities reflect a fundamental reality. The long-term sustainability of the NHS depends on a different model of care, one that is more personalised, proactive, preventative and equitable.

Emerging technologies have a critical role to play in enabling this shift. Artificial intelligence, advanced data infrastructure, cybersecurity and quantum technologies have the potential to improve clinical decision making, support earlier diagnosis, strengthen resilience and unlock new forms of biomedical discovery. However, technology alone will not deliver the change required. The challenge is whether health and care systems can build the capability to use these technologies safely, responsibly and at scale.

This means moving beyond technology adoption towards whole system readiness, that is the conditions that allow innovation to be adopted safely, governed responsibly, embedded into real pathways, trusted by the public, used well by the workforce and scaled where it delivers value. This question sat at the heart of the IGNITE Health Innovation Summit 2026, held in January as a collaboration between UCL and UCLPartners. The summit brought together senior clinicians, researchers, policy leaders, industry partners, innovation leaders and system stakeholders to explore the theme of “The Future of Health and Emerging Health Innovation”. Its value lies in creating a space where scientific possibility, clinical reality, policy ambition and implementation challenge can be considered together.

The summit considered emerging technologies through four critical lenses: technical feasibility, operational necessity, ethical responsibility and strategic value. Across the discussions, participants returned to a shared question: what kind of health system do we need to build to use emerging technologies well, and for the benefit of the people it serves?

A consistent theme was that innovation must be judged not only by technical performance, but by whether it improves access, reduces unwarranted variation and avoids widening existing inequalities. Technologies can support more personalised and preventative care, but they can also reinforce existing gaps if they are developed without people-centred co-creation, public trust and real-world implementation.

This report is organised around three interconnected domains of system readiness.

- **Clinical intelligence:**

how artificial intelligence, machine learning, digital twins and advanced decision support tools can augment clinical judgement, improve decision making and support multidisciplinary care.

- **Data, governance and cybersecurity:**

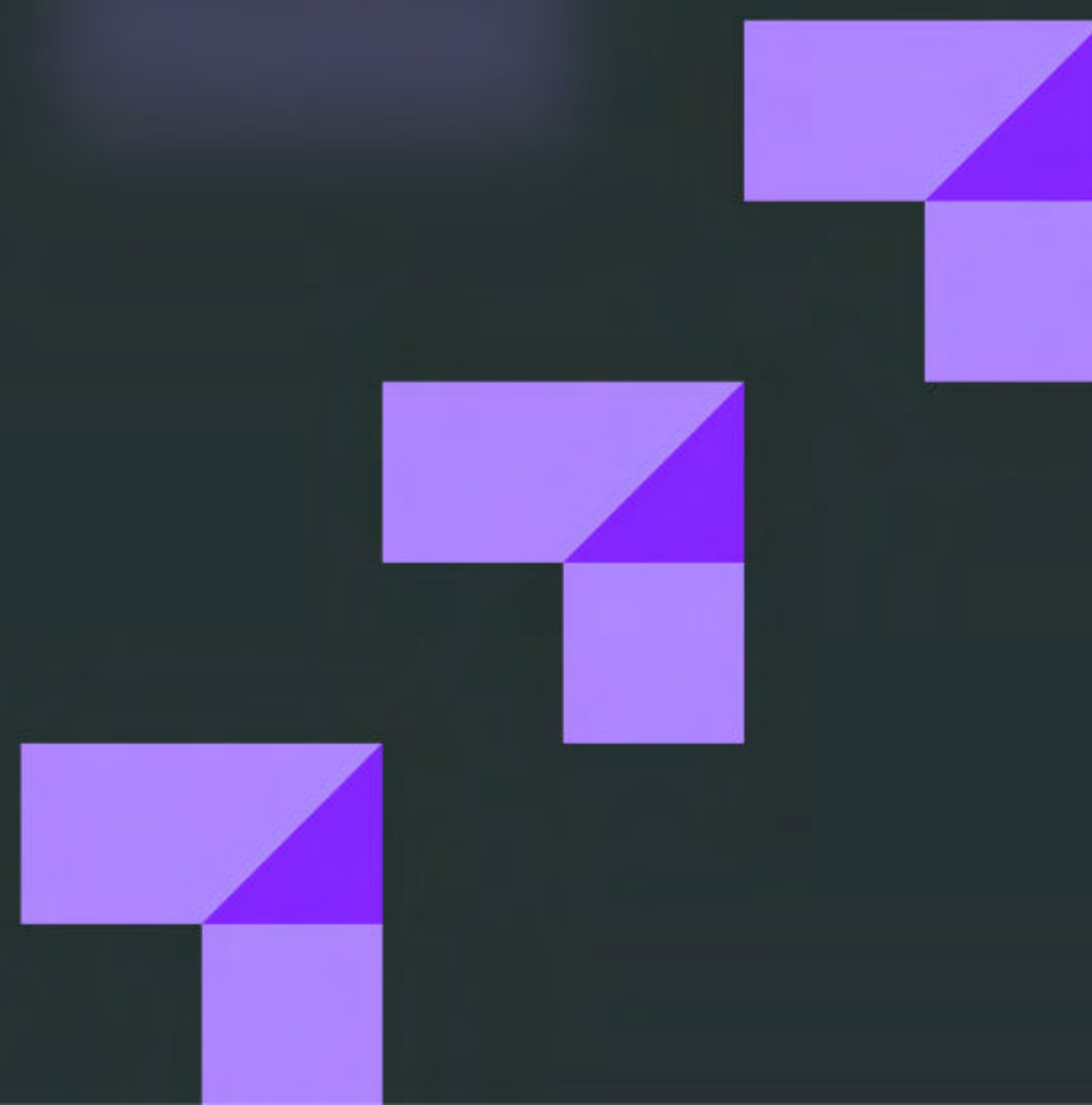
how health data can be used responsibly and securely, how governance can enable learning, and why cyber resilience must be understood as part of care delivery.

- **Quantum technologies in healthcare:**

how quantum sensing, quantum computing and post-quantum cybersecurity may affect diagnostics, biomedical research, precision medicine and long-term data security.

The report is intended for senior leaders across health and care, including providers, commissioners, policymakers, researchers, industry partners and innovation teams. It is designed to support strategic thinking and practical action by identifying the choices, capabilities and partnerships needed to translate emerging technologies into measurable benefits.

Senior leaders should therefore not simply ask which technologies they should develop, adopt and scale, but what kind of health system they are prepared to build. The system readiness test that follows turns this question into a practical framework for leadership action.

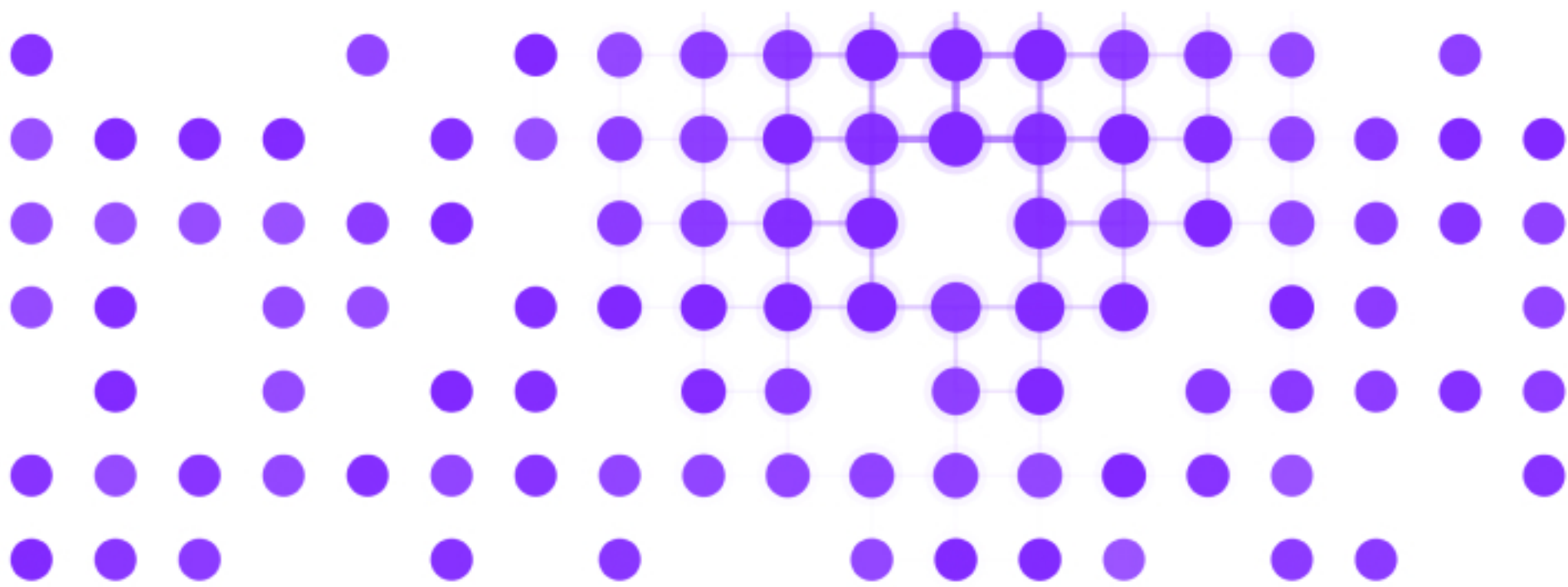


The system readiness test

The central question for health innovation is shifting. It is no longer enough to ask whether a technological solution is promising, accurate or novel. Health leaders must also ask whether the system is ready to adopt it and maximise its benefits.

The system readiness test turns this concept into a practical set of leadership questions. It is designed to help leaders assess the impacts, the opportunities and the risks before technologies are adopted, while they are being tested, and after implementation to understand whether they are delivering the intended impact.

Readiness condition	The question for leaders
Problem readiness	Has the clinical, operational, population or infrastructure need been clearly defined, or is the work being driven by technological novelty and hype?
Pathway readiness	Is it clear how the innovation fits into the pathway, who will act on the insight, what intervention follows and what outcome should change? Is the existing pathway fit for purpose, or does it need to be reimaged?
Value and equity readiness	What value is the innovation expected to create, for whom, and how will leaders know whether it improves outcomes, access, equity, productivity or patient and staff experience? Can it be sustained financially, operationally and environmentally beyond initial funding or pilot support?
Data and trust readiness	What data is needed to deliver public benefit, and how can this be used responsibly, transparently and with public confidence?
Workforce and workflow readiness	Are the relevant workflows understood, have staff been involved from the start, and have the required skills and capabilities been identified? How will the technology support staff, reduce burden and strengthen professional judgement?
Governance and accountability readiness	Are responsibility, assurance, validation, escalation, bias monitoring and post deployment surveillance requirements defined before implementation begins?
Implementation and resilience readiness	Can the system select, test, evaluate, procure and adopt the technology safely? Are the required digital, data, interoperability, commercial and supplier conditions in place? Can services recover from disruption, scale what works and stop what does not?
Horizon readiness	Is the system using foresight and futures thinking to anticipate emerging capabilities, risks and adoption choices before they become urgent? How are these insights shaping strategy, investment, partnerships and preparedness?



These conditions are connected. A technological solution may be technically strong but fail the readiness test if it does not address a real problem, cannot be embedded into workflow, lacks public legitimacy, places additional burden on staff or cannot be governed safely. Equally, a less complex tool may create significant value if it improves a critical decision, fits the pathway, earns trust and can be scaled reliably.

The readiness test reframes leadership responsibility. Innovation is a whole system task, extending well beyond digital, research or transformation teams. Clinical strategy, data governance, workforce development, public engagement, cyber resilience, procurement, evaluation and implementation all determine whether innovation succeeds or not. For senior leaders, the test is therefore direct:

Are we ready to use this innovation in a way that improves decisions, strengthens trust, supports staff, protects services and delivers measurable value for patients and populations?

It requires leadership discipline: the willingness to pause, redesign or stop innovations that fail to meet readiness conditions, and the ability to work across organisational boundaries where no single institution can deliver change alone.

The system readiness test is not a pass/fail exercise. If leaders cannot answer the readiness questions confidently and honestly, the appropriate response is not to proceed regardless, but to identify which conditions need strengthening before adoption or scale. The test's value lies in helping system leaders spot the factors that will enable or hinder implementation, and where additional support, partnership or capability is needed. Organisations such as UCLPartners can help leaders understand their system's strengths and weaknesses, and build the conditions for readiness.

The chapters that follow apply this readiness lens to three areas of emerging health innovation. Chapter 1 considers clinical intelligence and the need for decision-ready pathways, clear accountability, workflow fit and workforce confidence. Chapter 2 examines trusted data use, practical governance, cyber resilience and public legitimacy. Chapter 3 looks to the quantum horizon and the need for clinical pull, horizon scanning, test environments, adoption routes and post quantum security planning. Together, these domains show that the next phase of health innovation will depend on more than ambition. It will depend on whether health systems are ready to turn innovation into trusted, practical and scalable change.

1 **Clinical intelligence must be built around decisions**

Health systems are increasingly rich in data but still constrained by their ability to turn information into timely, trusted and actionable decisions. Clinical intelligence should therefore be judged not by the volume of insight it generates, but by whether it improves the decisions that shape care.

In this domain, system readiness means having decision ready pathways, clear accountability, workflow fit, trusted data, workforce confidence and feedback loops that show whether new tools are improving care in practice. It is not enough for health systems to adopt AI, analytics, digital twins or agentic systems. They must be ready to use them in ways that support clinical judgement, reduce burden, strengthen multidisciplinary working and improve outcomes for patients and populations.

When the system is not ready, innovation can create more complexity rather than more value. Predictive tools may identify risk without changing care. Dashboards may add information without improving prioritisation. Alerts may increase cognitive burden without supporting better action. AI outputs may influence decisions without clear accountability. Technologies may perform well in development but fail to scale because they do not fit real workflows, local populations or operational constraints.

The leadership challenge is therefore to move from clinical intelligence as a collection of tools to clinical intelligence as part of the operating model of care.

Better decisions, not more predictions

A common assumption in health innovation is that more data will inevitably lead to better care. In practice, this often overstates the value of data accumulation and understates the difficulty of acting on the insights produced. Clinicians already work in environments saturated with risk scores, alerts, dashboards, stratification tools, guidelines and performance metrics. The challenge is not simply the absence of intelligence, but the ability to translate intelligence into timely and appropriate action.

This matters in a system facing rising demand, increasing complexity of illness, workforce pressures and a growing need to shift care closer to home. In this context, decision making becomes a critical bottleneck.

A predictive model may identify risk accurately, but if no one is clear who should respond, what intervention is available, or how the insight fits into existing workflows, its impact will be limited. A dashboard that does not change prioritisation, or an alert that adds cognitive burden without changing care, risks becoming another layer of noise. As one participant commented

“decisions rather than data are the bottleneck. It is not only about having information, but also about making decisions based on potentially minimally relevant information.”

Decision readiness requires a shift from prediction to intervention. Accuracy remains important, but it is not sufficient. Clinical intelligence must help teams decide what should happen next: when to intervene, when to monitor, when to escalate, when to de-escalate and when not to act. In a pressured system, avoiding unnecessary intervention can be as valuable as triggering urgent action. The goal is better judgement, sharper prioritisation and more appropriate use of resources, rather than maximised activity.

This requires a more disciplined approach to data and model design. The value of a data element should not be judged only by whether it improves model performance. It should be judged by whether it reduces uncertainty enough to enable a better decision. The most useful models may not always be the most complex. In many cases, the system may gain more from tools that use the minimum meaningful information needed to support a high-quality decision, particularly where they are easier to interpret, govern and embed in practice. For executive leaders, this changes the starting point for innovation.

The question should not be “where can we apply AI?”, but “where are poor, delayed or inconsistent decisions creating harm, waste, inequity or avoidable demand?” Those decision points should become the priority areas for clinical intelligence. Leaders should ask whether a tool improves the quality, consistency, timeliness and equity of decisions. Does it support earlier intervention? Does it reduce unwarranted variation? Does it improve patient flow? Does it help teams use scarce capacity more effectively? Does it support prevention or appropriate watchful waiting? These are the tests that matter.

Designing decision-ready pathways for the realities of care

Clinical decisions are made in complex operational environments. They take place in multidisciplinary team (MDT) meetings, emergency departments, outpatient clinics, community services, virtual wards and care coordination hubs. They involve clinical evidence, professional judgement, patient preference, resource constraints and competing priorities across the system.

Clinical intelligence will only create value if it is designed for this reality. Tools that sit outside workflows, require additional data entry, produce outputs that are difficult to interpret, or fail to align with real decision points will struggle to scale. They may be technically impressive, but they will not become operationally useful.

This is particularly relevant for multidisciplinary teams. MDTs are central to decision making in complex care, but many are under increasing pressure. Discussions can be shaped by governance requirements, risk management, limited time and the need to reach consensus. Clinical intelligence should support MDTs by strengthening the structure, consistency and transparency of deliberation, complementing professional judgement rather than replacing it.

Decision support tools should therefore be designed as decision infrastructure. Their purpose is to help teams understand what is happening, anticipate what might happen and decide what should happen next. This requires tools that reduce cognitive burden, make uncertainty explicit, clarify trade-offs and support shared decision making across professional boundaries.

A decision-ready system is one in which the pathway around the tool is as carefully designed as the tool itself. Leaders should be clear about where the insight appears, who sees it, who acts on it, what intervention follows, how the decision is documented and how the outcome is reviewed. Without this operational clarity, clinical intelligence risks remaining peripheral to care, regardless of its technical sophistication.

Digital twins and agentic AI as decision augmentation

Digital twins and agentic AI point to a more advanced model of clinical intelligence. Digital twins create computational representations of patients, pathways or systems, allowing teams to simulate scenarios before acting. Rather than only predicting risk, they can help clinicians and leaders explore the likely consequences of different interventions.

One participant suggested that

“digital twin technology could enable MDTs to optimise decision making.”

At patient level, a digital twin could help compare potential care pathways and assess how different decisions may affect outcomes over time. At service or system level, simulation could help leaders understand how clinical decisions interact with patient flow, capacity, workforce and resource allocation. This creates the potential to test decisions before implementation, rather than relying only on retrospective evaluation.

Agentic AI may also play an important role. Unlike traditional tools that provide a single output, agentic systems can integrate evidence, guidelines, patient data and operational constraints across several stages of reasoning. Used well, they could act as thinking collaborators, helping clinicians compare options, structure deliberation and understand broader consequences.

However, these technologies must be positioned carefully. Their role is to augment and amplify clinical judgement rather than automate it. They should help teams ask better questions, surface uncertainty, consider alternatives and make more transparent decisions. The leadership task is to ensure that these tools strengthen human judgement rather than obscure it.

System readiness becomes especially important as these technologies become more powerful. The more advanced the tool, the greater the need for clarity about purpose, accountability, safety, escalation, workforce capability and real-world evaluation. Without these conditions, digital twins and agentic AI could increase dependence on opaque systems without improving the decisions that matter most.

Accountability for AI enabled decisions

As clinical intelligence becomes more embedded in decision making, system leaders and health professionals must establish clear accountability for AI enabled decisions. The critical issue is not only whether an AI tool, digital twin or agentic system produces a reliable output, but how that output is used, challenged and reviewed within clinical practice.

Accountability must be defined before tools are scaled. The operating model should be clear about who remains responsible for the final decision, how AI outputs inform rather than replace clinical judgement, and what responsibilities sit with clinicians, organisations, suppliers and system leaders. Without this clarity, there is a risk that responsibility becomes blurred, particularly when decisions are shaped by complex models or automated recommendations.

Validation and audit also need to be built into the operating model. Tools should be tested for their relevance to local populations, pathways and service contexts, as well as for technical performance. Their performance should be reviewed over time, including whether accuracy changes across different patient groups, clinical settings or patterns of use. Bias monitoring should be continuous, with clear processes for identifying whether tools are producing unequal benefits, reinforcing existing variation or creating new risks for underserved groups. AI enabled decision making also requires clear escalation routes.

Clinicians and teams need to know what to do when an AI output conflicts with clinical judgement, patient preference, operational reality or other sources of evidence. Tools should make uncertainty visible, enable challenge and allow decisions to be explained. The aim is not to remove professional judgement, but to make decision making more transparent, consistent and accountable.

Post deployment surveillance is essential. Health systems need to understand whether tools improve decisions in practice, not only whether they performed well during development. Review should examine whether AI supported decisions reduced time to intervention, improved prioritisation, supported appropriate watchful waiting, reduced unnecessary escalation, improved outcomes for underserved groups or created unintended consequences.

These feedback loops should be established from the outset, so that tools can be adapted, withdrawn or scaled based on real world impact. AI enabled decision accountability should therefore be treated as a core condition of clinical intelligence readiness. The question is not simply whether the system can use AI safely, but whether it can govern how AI influences decisions, learn from the outcomes of those decisions, and ensure that responsibility remains clear at every stage of care.

Workforce co-creation as a safety, usability and adoption requirement

Clinical intelligence is as much a human and organisational challenge as a technical one, shaped by people, workflows, culture and the realities of care delivery. Co-creation should therefore not be treated as an engagement exercise. It is a safety, usability and adoption requirement.

Clinicians and care professionals understand the decision points, risks, workarounds and pressures within pathways. Operational teams understand capacity, flow and implementation constraints. Patients and communities understand what matters for access, experience and trust. Without these perspectives, tools may solve the wrong problem, add burden, disrupt care or reinforce inequalities.

This means innovation must be driven by clinical and system needs. Frontline teams need clear routes to signal the problems that most need solving, and development should bring together clinicians, operational leaders, patients, communities, data scientists, AI researchers and industry partners from the outset.

The workforce challenge is therefore not only whether staff can use new tools, but whether they can shape, challenge and improve them. Leaders will need to build confidence in AI and data, create stronger clinical and technical collaboration, and develop roles that bridge clinical practice, analytics, operations and implementation.

A system is not ready for clinical intelligence if the workforce is expected to adopt tools that it has not helped shape, does not trust, cannot challenge or experiences as additional burden. Workforce readiness means giving staff the confidence, time, skills and authority to use clinical intelligence safely and improve it over time.

What leaders need to do now

1. Start with the problem or the decision needed, not the technology

Clinical intelligence should begin with the decisions that matter most, not with the technology available. Leaders should identify where poor, delayed or inconsistent decisions create harm, waste, inequity or avoidable demand, and make these the priority areas for AI, analytics, digital twins and decision support.

Every clinical intelligence project should be able to answer five questions: what decision is being supported, who will act on the insight, what intervention follows, what outcome should improve, and how will the system know whether the decision improved care? It should also identify the likely upstream and downstream consequences of implementation.

2. Build decision ready pathways

Decision support tools must be designed for the realities of care. This means developing tools with clinicians, operational teams, patients and communities from the outset, so that they fit workflows, reduce cognitive burden and support multidisciplinary decision making. Leaders should ensure that every tool is connected to a clear pathway. This includes defining where the insight is generated, how it enters workflow, who reviews it, what action follows, how uncertainty is handled and how decisions are recorded.

3. Establish accountability before scaling

Clinical intelligence should only be scaled where accountability is clear. Leaders must define responsibility for AI supported decisions, model validation, audit, escalation, bias monitoring and post deployment review.

Accountability should cover the whole lifecycle of the tool, from design and local validation through to implementation, monitoring, adaptation and withdrawal. This is essential for safety, public trust and professional confidence.

4. Build workforce confidence and capability

Leaders should invest in the capabilities required to use clinical intelligence well, including data and AI literacy, clinical and technical collaboration, and roles that bridge clinical practice, analytics, operations and implementation. Workforce confidence, usability and experience should be treated as core measures of success. A tool that performs well technically but increases burden, reduces trust or weakens professional judgement should not be considered ready for scale.

5. Measure real-world value

The value of clinical intelligence should be judged by whether it improves decisions in practice, not only by whether models perform well in development. Evaluation should include decision quality, workflow fit, usability, safety, equity, workforce confidence, patient outcomes and operational value.

Tools should be assessed against practical questions: did they reduce time to intervention, improve prioritisation, support appropriate watchful waiting, reduce unwarranted variation, improve outcomes for underserved groups or help teams use scarce capacity more effectively?

6. Create feedback loops for learning and improvement

Health systems should build feedback loops that connect decisions to outcomes. This will allow organisations to understand which decisions improved care, where unintended consequences emerged, and how practice should adapt over time. Readiness is a continuing capability where health leaders learn from implementation, improve tools in use, stop those that do not add value and scale those that demonstrably improve care.

Clinical intelligence will not transform healthcare by producing more insight alone. It will do so only when it helps the system decide better. That requires decision ready pathways, trusted data, accountable governance, workforce capability, resilient infrastructure and a clear focus on value for patients and populations.

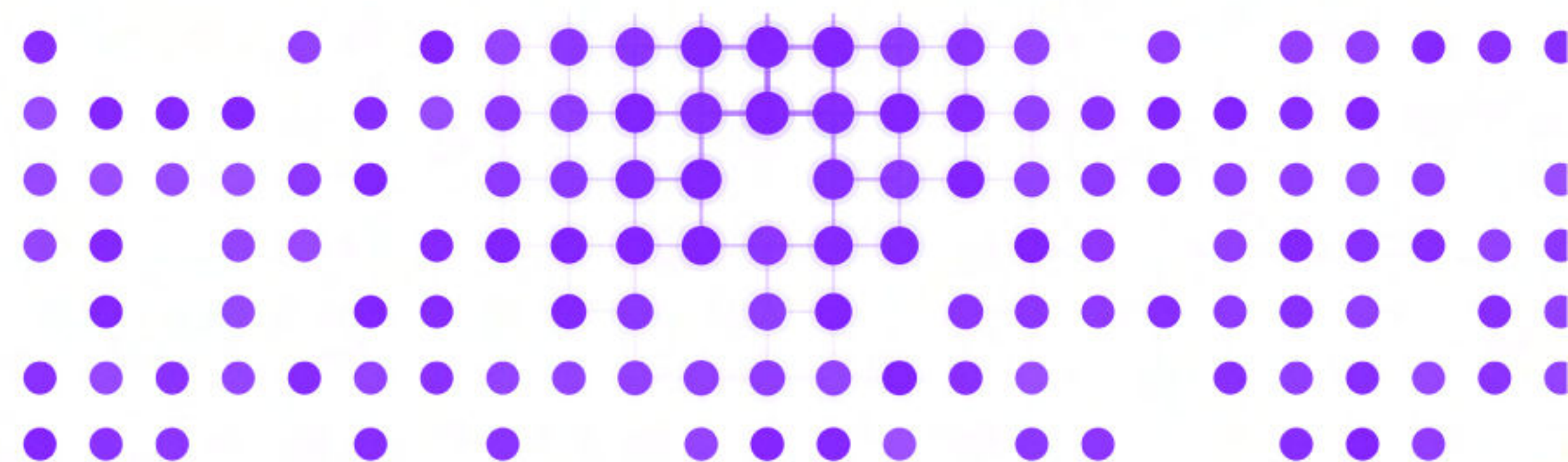
2 **Data governance must enable trust, learning and system resilience**

If clinical intelligence is to improve decisions, health systems need data environments that are trustworthy, well governed and resilient. Data governance can no longer be treated as a narrow compliance function. It is a strategic capability that determines whether innovation can move at pace, whether clinicians can access the information they need, whether the public trusts how data are used, and whether services can continue safely during digital disruption.

In this domain, system readiness means trusted data use, practical governance, cyber resilience and public legitimacy. It means having the confidence, safeguards, infrastructure and operating discipline to use data responsibly for care, research, planning, population health and continuous improvement. It also means being able to maintain safe services when digital systems, data flows or infrastructure are disrupted.

When the system is not ready, data and governance become a source of friction rather than learning. Governance processes can slow improvement, data sharing can become fragmented, public confidence can weaken, and cyber incidents can become patient safety incidents. Innovation then struggles to scale, not because the technology lacks potential, but because the system lacks the trust, clarity and resilience needed to use it well.

The leadership challenge is to create a system in which data can be used confidently, responsibly and purposefully. This means protecting patient information while enabling learning, managing risk while recognising the cost of missed insight, and treating cybersecurity as a service continuity priority rather than an information technology concern alone.



Governance must enable responsible data use

Health data governance has traditionally focused on controlling access, reducing risk and ensuring compliance with legal and regulatory requirements. These functions remain essential. Patients and the public must be confident that sensitive information is protected and used appropriately. However, governance that is experienced as complex, fragmented or overly defensive can become a barrier to the very improvements it is intended to support.

Across health and care, data sharing is often slowed by differing interpretations of information governance requirements, duplicated approvals and uncertainty about what is permissible. This can delay research, restrict service improvement, limit collaboration between organisations and make it harder to understand population needs. In a system seeking to move from treatment to prevention, from hospital to community, and from analogue to digital care, these barriers carry real opportunity costs.

The question is not whether governance should be strong, but whether it creates the clarity and confidence needed for responsible data use. Effective governance should enable appropriate data use across organisational boundaries while maintaining safeguards that are proportionate to risk. It should support professional judgement rather than displace it into excessive documentation and process. One participant suggested that

“you can’t change risk appetite without understanding and trust.”

Practical governance is therefore a core condition of system readiness. Policies, approvals and controls need to be clear enough for staff to use, consistent enough to support collaboration, and flexible enough to enable responsible innovation. Governance should not ask teams to choose between safety and improvement. It should create the conditions in which both are possible.

This requires governance to be designed with the people who must use it. Clinical leaders, operational teams, information governance specialists, cybersecurity experts, researchers, innovators and patients all need to be involved in shaping governance arrangements. Policies developed in isolation from operational reality risk creating friction, workarounds or delays. Governance that is clinically aligned and operationally practical is more likely to create confidence without creating unnecessary burden.

A learning health system needs minimum sufficient data

A learning health system depends on the ability to use data to understand what is happening, identify variation, test interventions and improve care over time. This requires a more mature approach than simply collecting as little data as possible.

Data minimisation remains an important principle. Health systems should not collect or use data without purpose. However, overly narrow interpretations of minimisation can unintentionally constrain learning. When datasets are too limited, the system may lose the ability to identify emerging patterns, understand inequalities, evaluate interventions or design better services. In these circumstances, the absence of data can itself create risk.

The more useful leadership concept is minimum sufficient data. This means identifying the data needed to support high-quality decisions, safe care, continuous learning, research, planning and improvement. It shifts the question from "how do we reduce data use?" to "what data are needed to deliver public benefit, and how can they be used responsibly?"

This matters especially for complex and vulnerable populations, including those supported across health and social care. People with multiple long-term conditions, frailty, mental health needs or social care requirements often interact with many parts of the system. Fragmented data can make their needs harder to understand and their care harder to coordinate. Responsible data use across organisational boundaries is therefore not only an innovation issue. It is an equity and quality issue.

Readiness for data enabled innovation therefore depends on the ability to balance risk and value. The risks of data use must be identified, managed and explained, but so must the opportunity costs of not using data. A learning system requires purposeful data use, transparent safeguards and clear accountability for public benefit.

For senior leaders, the task is to establish governance that enables the right data to be used for the right purposes, with the right protections, in ways that support care, learning and public confidence.

Public trust is an operating condition for data enabled healthcare

Public trust is a critical prerequisite for data enabled healthcare. Without it, patients may disengage from digital services, opt out of data sharing or question the legitimacy of innovation programmes. This can weaken research, reduce the representativeness of datasets and risk widening inequalities. Groups with lower trust may become less visible in the data used to design services, evaluate interventions and train future tools.

Trust cannot be solved through communications alone. It must be built into the operating model. People need to understand how their data are used, why this matters, what safeguards are in place and how data use benefits patients, communities and the wider system. Transparency is not simply about publishing information. It is about making choices visible, understandable and accountable.

This requires a shift from one off consultation to sustained public dialogue. Deliberative engagement, citizens' panels, patient forums and clear public facing information can help create more informed debate about data use. When people are asked about data sharing in abstract terms, they may understandably express caution. When the potential benefits, safeguards and governance arrangements are explained clearly, views can become more balanced and informed.

Public legitimacy is therefore part of system readiness. Health systems cannot assume that data use will be trusted simply because it is lawful, technically secure or clinically valuable. Trust grows when the system demonstrates that data use is transparent, proportionate, ethical and connected to real improvements in care.

Health systems should therefore treat trust as core infrastructure for innovation.

Public engagement should not be an afterthought once data programmes are already designed. It should shape the purposes, safeguards and accountability arrangements from the outset. The public should be able to see how data are protected, and equally, how that data use contributes to better care, fairer access and stronger services.

Cyber resilience is a patient safety priority

Digital infrastructure is now part of the clinical infrastructure of care. Electronic health records, diagnostic systems, prescribing platforms, communication tools, remote monitoring and operational dashboards all support day to day clinical decision making. When these systems are disrupted, care can be delayed, records may become inaccessible, services may lose coordination and patient safety can be affected.

Cybersecurity must therefore be understood as more than a technical or compliance issue. It is a core component of system resilience, concerned as much with keeping services running safely through disruption as with preventing attacks in the first place. As noted by one participant

“if cybersecurity is an issue, then it’s everybody’s issue.”

This requires board level ownership. Cyber risk should be visible in clinical risk management, emergency preparedness and operational planning. Leaders should understand the tradeoffs involved in cybersecurity decisions, including the relationship between security controls, usability, interoperability, workflow burden and patient flow. Perfect security is not achievable. Resilience depends on identifying the most critical risks, implementing proportionate safeguards and maintaining the capability to detect, respond and recover.

Operational preparedness is essential. Organisations should run regular downtime exercises, test alternative workflows and ensure that staff know how to maintain critical services when digital systems are unavailable. Cyber resilience should be rehearsed in the same way as other major operational and continuity risks. The question is not only whether systems are protected, but whether the organisation can continue to care for patients safely when systems fail.

A system is not ready for digital innovation if it becomes more dependent on data and technology without strengthening its ability to withstand disruption. Cyber resilience is therefore not separate from innovation. It is one of the conditions that allows innovation to be trusted, adopted and sustained.

Practical assurance, not performative compliance

Boards should not ask only whether policies, training, dashboards and compliance returns are in place. They should ask whether governance and resilience work in practice.

Formal controls are necessary, but they can create false assurance if they are not tested against the realities of care delivery. A completed training programme does not necessarily mean staff know what to do under pressure. A policy does not guarantee consistent behaviour across teams. A dashboard may show activity, but not whether controls are understood, usable or effective in clinical and operational settings.

Senior leaders therefore need assurance that goes beyond evidence of process.

They need to understand whether governance supports timely data use, whether staff can apply agreed procedures, whether controls create unintended workarounds, and whether services can continue to operate safely when systems, data flows or decision pathways are disrupted.

Board level assurance should include practical tests of how governance works in real conditions. Leaders should ask whether data sharing processes support safe and timely care, whether staff understand their responsibilities, whether public concerns are being addressed, whether critical services have been tested under disruption scenarios, and whether learning from incidents leads to change.

The aim should be practical assurance, not performative assurance. Governance should give boards confidence that the system is not only compliant on paper, but safe, trusted, resilient and able to learn in practice.

What leaders need to do now

1. Start with the problem governance needs to solve

Data governance should begin with the needs of patients, clinicians, researchers and system leaders, not with process alone. Leaders should identify where fragmented governance, unclear data sharing or overly defensive interpretation of rules is limiting care coordination, research, innovation or service improvement.

Every data governance programme should be able to answer four questions: what purpose does the data use serve, what public benefit will it enable, what risks need to be managed, and what safeguards are needed to maintain trust? The aim should be governance that protects patients while enabling responsible learning and improvement across organisational boundaries.

2. Build practical governance for trusted data use

Health systems should move towards a minimum sufficient data model. This means defining the data needed to support high-quality decisions, safe care, continuous learning, research, planning and population health, while ensuring safeguards are proportionate, transparent and trusted.

Governance processes should be co-designed with clinical, operational, information governance, cybersecurity, research and patient perspectives. This will help ensure that policies are practical, understood and aligned with real care delivery.

Leaders should also reduce unnecessary variation in local interpretation where it creates friction or delay. The goal is not weaker governance, but clearer governance that enables responsible action.

3. Treat public legitimacy as a core readiness condition

Trusted data use must be built into the operating model. Leaders should support ongoing public dialogue, clear patient-facing information and transparent explanations of how data are used, why they matter and what safeguards are in place.

Public engagement should shape data programmes before decisions are fixed. This will help ensure that data use reflects public expectations, addresses concerns and demonstrates visible benefits for patients and communities.

Boards should ask whether mistrust, opt outs or lack of understanding are affecting the quality, representativeness or legitimacy of data enabled innovation.

4. Govern cyber resilience as part of care delivery

Cyber resilience should be treated as a patient safety and service continuity priority. Boards should ensure that digital disruption is planned for, tested and governed with the right protocols in place.

This includes regular downtime exercises, clear recovery plans, tested alternative workflows and assurance that frontline teams know how to maintain critical services when systems are unavailable.

Leaders should also ensure that cyber risk is connected to clinical risk, operational resilience, emergency preparedness and supplier management.

5. Measure whether governance works in practice

The success of data governance should not be measured only by compliance activity. Leaders should assess whether governance enables timely data access, supports cross organisational collaboration, improves care coordination, strengthens research and maintains public confidence.

Boards should ask whether data sharing processes support safe and timely care, whether public concerns are being addressed, whether controls are creating workarounds, and whether governance is enabling learning across the system.

Practical assurance should test whether the system can use data responsibly in real conditions, not only whether policies and processes exist.

6. Build feedback loops for trust, learning and resilience

Health systems should learn continuously from data use, public engagement, cyber incidents, near misses and implementation experience. These feedback loops should inform governance, workforce training, public communication, technical controls and service design.

Readiness is a continuing capability, to use data wisely, maintain public confidence, strengthen resilience and adapt as risks, technologies and public expectations change, well beyond a one-off compliance threshold.

Data governance must become part of the operating model for a learning, trusted and resilient health system. The task is to ensure that data can be used wisely, transparently and securely, so that insight can translate into better care, stronger public trust and safer services. The future of data enabled healthcare will depend not only on what data the system holds, but on whether it can use those data responsibly, practically and resiliently.

3 **Quantum technologies in healthcare require strategic preparation**

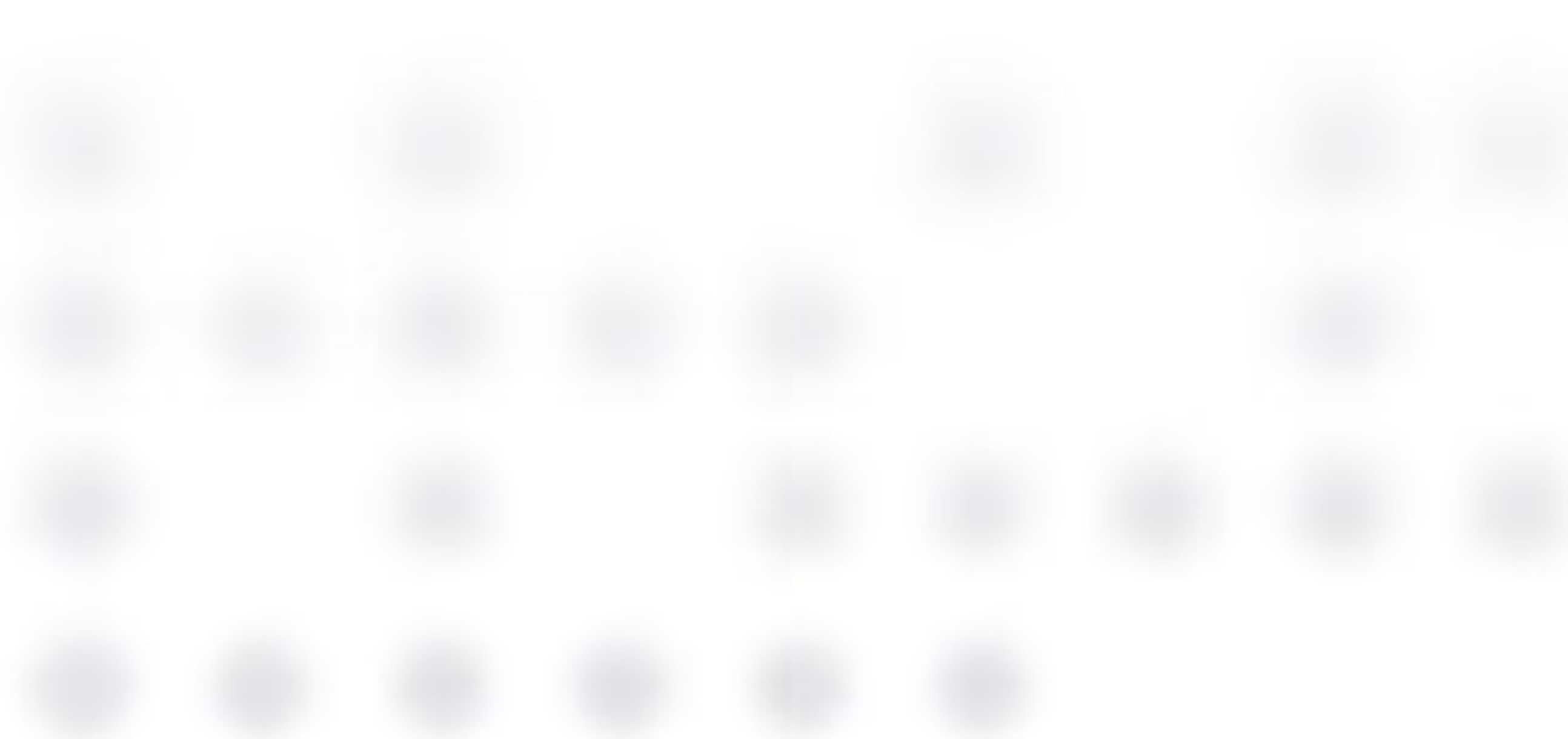
As health systems become more data dependent, quantum technologies present both an opportunity and a risk. Quantum sensing could enable more sensitive and portable diagnostics. Quantum computing may, over time, support new forms of biomedical modelling and discovery. Post quantum cybersecurity is already relevant, as sensitive health, genomic and research data may need to remain secure for decades.

In this domain, system readiness means clinical pull, horizon scanning, test environments, adoption routes and post quantum security planning. It means preparing early enough to shape quantum technologies around real clinical, research and infrastructure needs, rather than waiting for them to arrive fully formed. It also means recognising that different quantum technologies will mature across different timelines and will require different leadership responses.

When the system is not ready, quantum innovation risks following a familiar pattern. Promising technologies may remain trapped in research settings, disconnected from clinical workflows, evaluation requirements, procurement routes and service priorities. Technical possibility may move ahead of clinical demand. Health systems may also become exposed to future security risks if they fail to prepare for the implications of quantum computing for long lived sensitive data.

The case for preparation is therefore practical rather than speculative. Healthcare is becoming more digitally dependent, analytically complex and reliant on longitudinal data. The question is not whether quantum technologies are ready to transform care tomorrow, but whether health systems are preparing early enough to influence their development, evaluate their value and protect against future risks.

This means preparing across three horizons: nearer term opportunities in quantum sensing, longer term potential in quantum computing, and immediate action on post quantum cybersecurity.



Quantum is a strategic horizon for health and care

For many health leaders, quantum can seem distant from day-to-day service pressures. Yet the adoption challenge is already familiar. Promising technologies often fail to scale, not because the science is weak, but because the system is not ready to adopt them. The gap between discovery and deployment is created by unclear clinical demand, limited testing environments, fragmented evaluation routes, complex procurement and insufficient connection between researchers, clinicians, industry and system leaders.

Many participants noted that

“bridging the gap between clinicians and innovators is crucial to developing quantum solutions that will be most helpful.”

These barriers will apply to quantum unless preparation starts early. The priority is to build the partnerships, capabilities and adoption pathways needed for responsible use when these technologies become clinically viable, not to predict the exact timing of quantum maturity. Quantum readiness therefore begins with horizon scanning.

Leaders need to understand which quantum capabilities are likely to become relevant to health and care, what problems they may help solve, what risks they introduce, and what infrastructure, skills and partnerships will be needed. This does not require every organisation to become a quantum expert. It does require health systems to become informed customers, partners and shapers of emerging capability.

The leadership task is to ensure that quantum is not treated as either distant science or immediate hype. It should be positioned as part of a longer-term innovation portfolio, connected to clinical strategy, research priorities, digital infrastructure, data governance and cyber resilience.

Quantum sensing offers the nearer term opportunity

Quantum sensing is likely to offer some of the earliest practical opportunities for healthcare. It uses quantum properties of matter and light to measure physical signals at extremely small scales. In clinical terms, this could enable diagnostic tools that detect subtle biological signals with greater sensitivity, speed or portability than many current technologies.

The strongest near term potential is likely to come from applying quantum sensing to existing diagnostic challenges, rather than searching for entirely new problems. Health systems should ask where greater sensitivity, portability or earlier detection would change care. This may include diagnostics for neurological conditions, cancer detection, ophthalmology, physiological monitoring and community based screening.

For example, quantum sensors are being developed to detect very small magnetic fields produced by neural activity in the brain, which could support new approaches to neurological assessment and monitoring. In oncology, quantum enabled techniques may help identify subtle biochemical signatures in tissue. In ophthalmology, more portable diagnostic tools could support retinal imaging and screening outside specialist hospital settings, helping to move care closer to communities and reduce barriers to access.

The strategic value of quantum sensing is therefore not only technical precision. It is the possibility of changing where and when diagnosis happens. More portable, sensitive and accessible tools could support earlier intervention, strengthen prevention and enable care to move closer to home. This aligns directly with the direction of travel for health and care, particularly the shift from hospital centred models towards community based and preventative care.

However, readiness matters because more measurement is not automatically better care. Quantum sensing may generate richer and more frequent physiological data, but its value will depend on whether those signals lead to better decisions. Health systems will need clear clinical pathways, trusted data governance, workforce capability and implementation support. Without these conditions, new forms of measurement could add complexity, increase burden or create uncertainty without improving outcomes.

For leaders, the key question is not simply “what can quantum sensing detect?”, but “where would better detection change care, who would act on the result, and what pathway would support that action?”

Quantum computing is a longer term strategic horizon

Quantum computing is not yet mature for routine healthcare use, but its potential is significant. Over time, it may enable new approaches to analysing complex biological systems, modelling molecular interactions and solving optimisation problems that are difficult for classical computers.

This could have important implications for drug discovery, biomedical simulation and precision medicine. However, quantum computing should not be overpromised as an immediate answer to current operational pressures. Its pathway to impact is likely to depend on research partnerships, specialist infrastructure, technical expertise and clear use case development.

The leadership response should be strategic readiness. Health systems should horizon scan, build relationships with academic and industry partners, and identify where quantum computing could address genuine biomedical or system challenges. It should be treated as part of a longer term innovation portfolio, not as a near term operational fix.

Readiness for quantum computing means creating the conditions for future value before the technology is ready for routine deployment. This includes identifying biomedical questions where quantum approaches may eventually offer advantage, building links with research and industry partners, understanding infrastructure implications, and ensuring that future use cases are shaped by clinical and scientific value rather than novelty alone.

The risk of not preparing is that health systems become passive recipients of future technologies, rather than active shapers of their development. Without early clinical and research input, quantum computing may evolve around technical possibility without sufficient connection to the problems that matter most for health and care.

Post-quantum cybersecurity is an immediate leadership issue

While some clinical applications of quantum technology may take time to mature, the cybersecurity implications require attention now. Healthcare systems hold some of the most sensitive data in society, including medical records, genomic information, imaging, research datasets and linked population health data. Much of this information needs to remain confidential for decades.

Current encryption approaches rely on mathematical problems that are extremely difficult for classical computers to solve. Sufficiently powerful quantum computers could, in the future, make some existing encryption methods vulnerable. This creates a strategic risk for health systems, particularly because malicious actors may collect encrypted data today with the intention of decrypting it later, a risk often described as “harvest now, decrypt later”.

This is not a theoretical concern for future technologists alone. It is a board level data protection, cybersecurity and infrastructure planning issue. Health systems need to understand where long lived sensitive data are held, how they are protected, and what transition planning is required for post quantum cryptography. The shift to quantum resistant security standards will require time, investment, technical expertise and coordinated governance.

One participant noted

“there is a big onus to move to new encryption protocols now even though quantum computing is still developing.”

For leaders, the implication is clear. Digital health infrastructure must be future proofed. Cybersecurity strategies should anticipate technological change rather than react to it after vulnerabilities emerge. Post quantum readiness should be integrated into wider cyber resilience planning, particularly for systems that hold genomic, clinical and research data with long term sensitivity.

A system is not ready for the next phase of digital health if it is building greater dependence on sensitive data without planning for how those data will remain secure over time. Post quantum security planning should therefore be treated as part of system resilience, not as a specialist technical issue that can be deferred.

Quantum readiness means creating clinical pull early

The adoption challenge for quantum will be to create clinical pull before technologies are fully mature. Without clear demand signals from the health system, quantum innovation risks being shaped by technical possibility rather than clinical value.

Because quantum sensing, quantum computing and post quantum cybersecurity are developing across different timelines, each will need a different route to adoption. What they share is the need for early clarity about the healthcare problems they are intended to solve. For quantum sensing, leaders should identify where greater sensitivity, portability or earlier detection would materially change clinical pathways, such as neurological assessment, cancer diagnostics, ophthalmology, physiological monitoring or community based screening.

For quantum computing, the priority is to define biomedical questions where new computational approaches may eventually offer advantage, including molecular modelling, drug discovery, complex simulation and precision medicine. For post quantum cybersecurity, the task is to identify long lived sensitive datasets, critical systems and supplier dependencies that may require transition planning.

Quantum adoption should be guided by use cases that are clinically meaningful, technically plausible and operationally relevant. Early partnerships between clinicians, researchers, industry, patients, cybersecurity specialists and system leaders will be essential to shape emerging capabilities before design choices become fixed.

The aim is to avoid a familiar failure pattern in health innovation, where promising technologies remain trapped in research settings because they are not aligned with clinical workflows, evaluation requirements, procurement routes or service priorities.

Strategic preparation should therefore include test environments, early evaluation pathways and clear routes through regulation, health technology assessment, procurement and implementation.

The task goes well beyond investing in the science itself: it is to ensure quantum capabilities are pulled towards the problems that matter most for health and care.

Test environments and adoption routes will be critical

Quantum technologies will need safe places to be explored, tested and evaluated before they can be adopted at scale. This is especially important because their value will depend not only on technical performance, but on clinical relevance, usability, infrastructure requirements, cost, safety, equity and workflow fit.

Test environments should bring together clinicians, researchers, patients, operational teams, industry partners, data specialists and implementation experts. Their purpose should be to assess whether quantum-enabled tools solve meaningful problems in real conditions, and whether they can be integrated into pathways without increasing burden or widening inequalities.

Clear adoption routes will also be needed. Innovators will need to understand how quantum technologies move through evidence generation, regulation, health technology assessment, procurement and implementation. Health systems will need mechanisms to stop weak propositions early and accelerate those with the strongest clinical value, usability and implementation potential.

Without these routes, quantum innovation may become fragmented. Individual pilots may emerge, but they may struggle to move into routine use. Readiness therefore depends on building the implementation infrastructure before demand becomes urgent.

What leaders need to do now

1. Start with the clinical, research or strategic need

Quantum activity should begin with clear clinical, research or infrastructure needs, rather than technology curiosity. Leaders should identify where greater sensitivity, portability, computational capability or long-term data security could address a meaningful problem in care, research or system resilience.

Every quantum use case should be able to answer four questions: what problem is being addressed, why quantum may offer an advantage, what pathway or infrastructure would need to change, and what value would need to be demonstrated before adoption?

Quantum sensing, quantum computing and post quantum cybersecurity should be considered through different time horizons, with near term focus on sensing, longer term focus on computing, and immediate action on data security.

2. Build the enabling conditions for quantum readiness

Health systems should develop a quantum readiness roadmap that distinguishes between near term, medium term and long term opportunities. This should include horizon scanning, clinical use case development, test environments, post quantum cybersecurity planning and links to wider NHS infrastructure and adoption strategies.

The roadmap should identify where quantum technologies could support earlier diagnosis, more accessible testing, better monitoring, faster discovery, stronger data protection or more equitable access to care. It should also clarify which actions need to begin now, which capabilities require partnership, and which areas should be monitored as the science and market mature.

3. Create clinical pull through early partnerships

Quantum capability will require partnerships across healthcare, academia, industry and national infrastructure. Leaders should build relationships across physics, engineering, computer science, clinical practice, data science, regulation and implementation.

These partnerships should not be limited to technical development. They should help define the clinical and operational problems quantum technologies are intended to solve, the evidence needed for adoption, and the conditions required for safe and equitable implementation.

Patients and communities should also be involved where quantum enabled tools may change diagnostics, monitoring, data use or access to services.

4. Establish test environments and evaluation routes

Leaders should support test environments where early prototypes can be evaluated safely with clinicians, patients and operational teams.

These environments should assess not only whether quantum technologies work technically, but whether they are clinically useful, operationally feasible and trusted by users. Early evaluation should include clinical relevance, workflow fit, patient and workforce impact, safety, equity, cost, infrastructure requirements and adoption readiness.

The purpose should be to create evidence that helps leaders make informed decisions about whether to scale, adapt or stop emerging technologies.

5. Prepare now for post quantum cybersecurity

Post quantum cybersecurity planning should begin now, particularly for systems holding sensitive health, genomic and research data that must remain secure for decades. Leaders should identify long lived sensitive datasets, critical systems, supplier dependencies and areas where encryption transition planning may be required.

This should be integrated into wider cyber resilience, data protection, infrastructure and procurement strategies. Boards should seek assurance that future security risks are being considered as part of digital transformation, not treated as a distant technical issue.

6. Build adoption routes from discovery to deployment

Quantum technologies will need clearer routes from discovery to deployment. Adoption pathways should help innovators navigate regulation, health technology assessment, procurement and implementation. Health systems should also ensure that adoption decisions are guided by clinical need, public value, workforce impact, equity and resilience, not novelty alone.

The task now is to shape these technologies while they are still forming, rather than adapt to them once they've already arrived. The leadership task is not to wait for quantum technologies to arrive fully formed, but to build the readiness to shape them around clinical need, protect against future security risks and adopt them responsibly.

Quantum readiness means preparing early enough to ensure that future capability is pulled towards the problems that matter most for patients, communities, staff and the wider health system.

Conclusion

The IGNITE Summit 2026 revealed a clear leadership challenge. Scientific and technological progress is accelerating, but its value for health and care will depend on whether systems are ready to turn possibility into disciplined, trusted and practical change.

The issue is no longer whether emerging technologies have potential. They do. The harder question is whether health and care systems have the readiness to use them well. That means being able to define the right problems, build decision ready pathways, govern data responsibly, maintain public trust, support the workforce, withstand digital disruption and create clear routes from discovery to adoption.

This is the shift from innovation ambition to system readiness. Ambition is essential, but it is not enough. Health systems will not realise the value of AI, data infrastructure, cybersecurity or quantum technologies simply by adopting new tools. They will realise value when those tools are shaped around clinical need, embedded into real workflows, supported by trusted governance, evaluated in practice and scaled where they demonstrably improve care.

Across the summit discussions, three readiness challenges stood out. First, clinical intelligence must improve decisions, not simply generate more information. Health systems need decision-ready pathways, clear accountability and feedback loops that show whether AI, analytics and digital twins are improving outcomes, reducing variation and supporting staff. Second, data enabled innovation depends on trust, practical governance and resilience. Data must be used wisely and transparently, and digital infrastructure must be treated as part of safe care delivery. Third, emerging horizons such as quantum technologies require preparation now. Leaders need clinical pull, horizon scanning, test environments, adoption routes and post quantum security planning before these capabilities become urgent.

This is a shared responsibility. Policy leaders need to reduce friction across evaluation, regulation, procurement and adoption. Providers need to create the conditions for safe testing, implementation and learning in real care settings. Academic partners need to connect discovery more deliberately to clinical and population needs. Industry needs to design for evidence, usability, interoperability, equity and trust from the outset. Patients, communities and the workforce must also be involved in shaping the purposes, safeguards and conditions for innovation. None of these actors can deliver the next phase of health innovation alone.

The risk of inaction is significant. Without stronger system readiness, promising technologies will continue to be unevenly adopted, poorly integrated or disconnected from the needs of patients and staff. Services may become more dependent on digital and analytical capabilities without the confidence, governance, skills and resilience required to use them well. In that scenario, innovation could increase variation rather than reduce it, add burden rather than release capacity, and weaken trust rather than build it.

The cross cutting implication is clear. Clinical strategy, data use, workforce development, public engagement, digital resilience, implementation infrastructure and research translation are now part of the same leadership task. Progress will depend on institutions that can work across boundaries, learn from implementation and make explicit choices about the future they are trying to build.

The call to action from IGNITE is direct. Senior leaders must move beyond interest in emerging technologies and take responsibility for the conditions that allow them to deliver value. They should ask not only what technologies are available, but whether their systems are ready to absorb, govern, implement, evaluate and scale them in ways that improve care.

The next phase of health innovation will not be defined by the novelty of the tools available. It will be defined by the readiness of health systems to shape those tools around the needs of patients, communities and the workforce. The opportunity is substantial, but it will not realise itself. IGNITE Summit 2026 has shown what is possible. The task now is to build the system readiness required to move beyond isolated innovations and deliver transformation at scale.