celerity | IBM Platinum Partner | GOV.NEWS

Quantum Ready:

Securing Data in the NHS

Contents

Introduction

The NHS faces a silent threat that no one is talking about. Quantum computing offers transformative potential, but it also presents risks, regardless of whether you use it as an organisation.

Experts are concerned about threats to data security. The power of quantum computers will make encryption easy to crack, leaving sensitive patient data vulnerable. Even if your NHS organisation doesn't use quantum, criminals are banking on it. Critical infrastructure is at risk.

The threat is closer than you think. Bad actors are already harvesting data so that it can be decrypted (unlocked) when they have access to quantum computing. The time to act is now. NHS trusts need a plan to protect patient data.

The next quantum advance could happen at any time. No longer the domain of labs, breakthroughs are happening here and now. Google unveiled a chip that takes five minutes to solve a problem that would take the world's fastest computers ten septillion years[1] Tech giant Amazon's announcement of a quantum breakthrough signals that the race is on.[2] With big business backing, advances will only accelerate.

NHS leaders need to understand the urgent risks and opportunities to develop a quantum-ready strategy. Now is the time to start taking action to keep your data safe.

So how can you become quantum-ready and protect NHS data?

Data Security Risks

As the custodian of sensitive patient data, the NHS is likely to be a target of bad actors. Organisations face several data security challenges:

Lack of data visibility

Many organisations struggle to track where sensitive data is, how it moves and who has access. Cloud and generative AI have complicated the picture and blocked data visibility.

Evolving cyber threats

Cyberattacks are increasing in sophistication and impact. The rise of ransomware, AI-enhanced attacks and advanced persistent threats (APTs) all threaten sensitive data. Traditional security is no longer enough.

Governance requirements

NHS organisations are looking to harness data to support a shift to proactive, predictive care while navigating rigid governance requirements.

Decrypting sensitive information

The arrival of quantum poses security risks. The BBC reports that 'the arrival of quantum computing means that many of the encryption algorithms that underpin and secure our hyperconnected world will be trivially easy to crack.'[3]

Growing insider threats and vulnerabilities

Human error, unauthorised access, and social engineering can lead to the exfiltration of sensitive data. Vulnerabilities are multiplied by complex supply chains.

As we enter a new era, data and digital transformation will be the lifeblood of the NHS. Leaders need to adapt to survive and thrive in a rapidly evolving environment. Patient safety depends on securing data and becoming quantum-ready.

A Changing Landscape

At the same time as the environment is evolving rapidly, the NHS is undergoing significant change. Leaders need to set the direction in line with several strategic drivers without losing sight of data security risks:

The three big shifts

The government is committed to three big shifts in the NHS: moving care from the hospital to the community, from treatment to prevention, and from analogue to digital.[4] The Prime Minister suggested the need for the NHS to be a 'tomorrow service, not just a today service.'[5]

The Lord Darzi review

Lord Darzi's rapid investigation into the state of the NHS concluded that 'the NHS is in critical condition, but its vital signs are still strong.' It called for transformation, including a 'tilt towards technology' to unlock productivity.[6]

Data Saves Lives

This strategy highlights the power of data to save lives. Leaders must build trust and create the right foundations to maximise opportunities to enhance patient care.[7]

The Cyber Security Strategy

Cyber resilience is a key driver. The London cyberattacks in 2024 highlighted the vulnerability of NHS systems in a rapidly evolving landscape.[8] NHS leaders need to keep pace with the changing environment to keep patient data safe.

The government's quantum strategy

The government's recent £121 million investment in quantum signals its commitment to the industry. Yet the strategy focuses on supporting the growth of quantum-enabled businesses rather than mitigating the risks to the public sector.

The lack of an NHS quantum strategy

The current lack of an NHS quantum strategy represents a blind spot. The sector risks getting left behind due to gaps in skills, capabilities and expertise. Without action now, sensitive patient data will be vulnerable.

Decoding quantum

So, what do we mean by quantum? Essentially, classical computing relies on a binary system, while quantum uses qubits, which can occupy multiple positions. Computing power multiplies - the possibilities are almost limitless.

Companies are investing heavily in quantum because of the technology's augmented capabilities. The government has signalled its intent with a £121 million investment to scale quantum in the UK.[9]

Quantum computers will solve complex problems in a matter of minutes. Traditional computing will become obsolete almost overnight. As advances gather pace, the technology will no longer be the preserve of the lab, but will become mainstream.

While the technology isn't there yet, advances are happening all the time. We may be on the edge of a breakthrough.

A quantum leap

The arrival of quantum will revolutionise patient care. Drawing on rich NHS data, it will be possible to make new connections and surface rich insights. Quantum's problem-solving abilities could lead to breakthroughs in the NHS. A quantum leap.

Progress is accelerating. The multi-million investment in quantum hubs signals the size of the opportunity for the NHS. The University of Birmingham is one of the UK's trailblazers. It's trialling quantum brain scanners to enhance diagnosis and patient care.[10]

Quantum is no longer the preserve of the future. Leaders need to act now to maximise opportunities and mitigate risks.

New threats

Quantum not only multiplies possibilities – it also multiplies threats. Traditional security relies on encryption as the line of defence against bad actors. But it's not enough to safeguard against quantum-powered attacks.

Quantum computing has the power to expose encrypted data. In an NHS context, this could be commercial or financial information, personal staff details and patient records. Data exposure could result in denial of service, data loss, and data theft. The impact could be far-reaching. There's a real threat of widespread disruption, reputational damage, financial losses and risks to patient safety.

Advances in quantum are not just a niche IT issue. They're a strategic risk that must be owned at a board level.

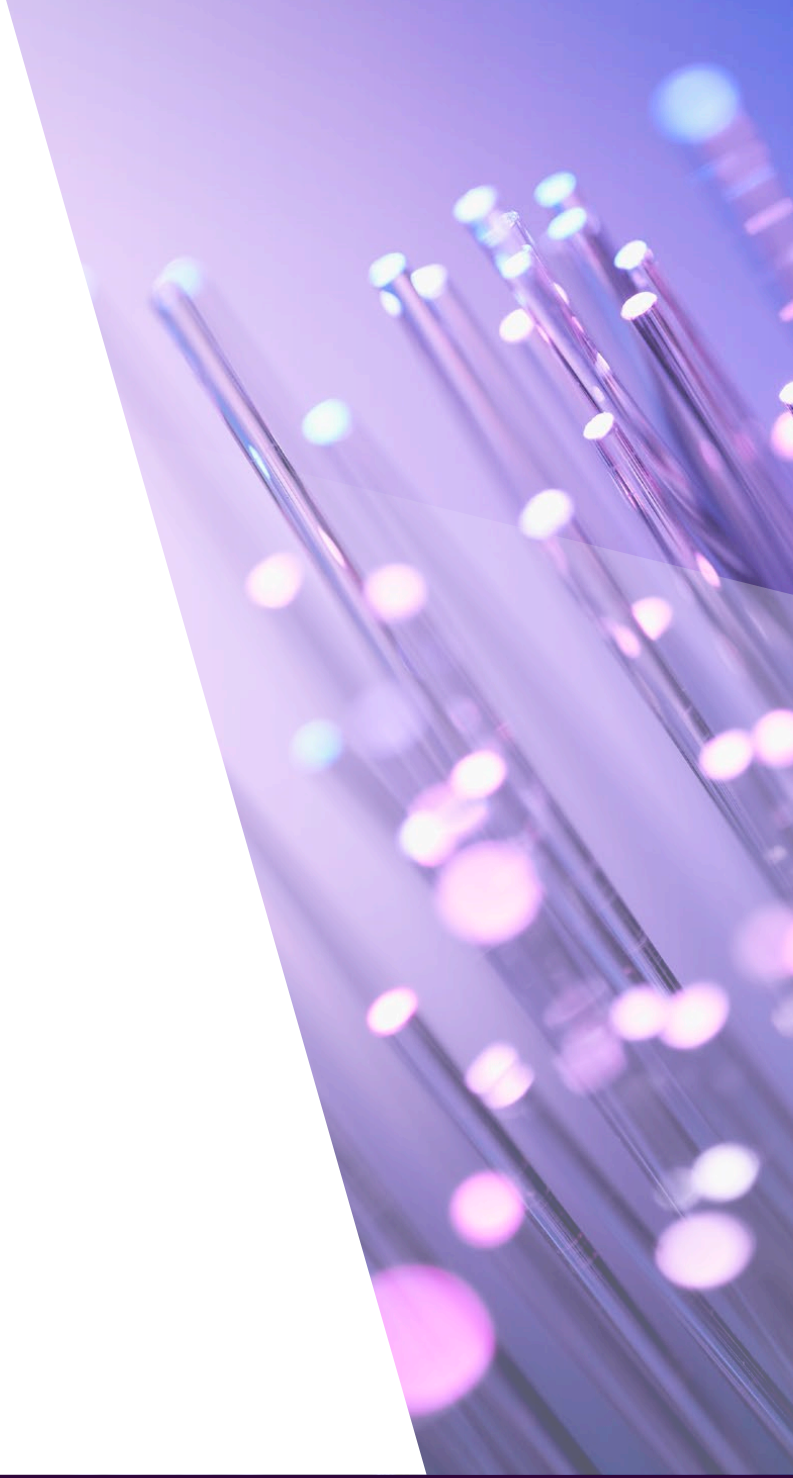
Q Day

Cybersecurity experts warn about the impact of Q Day. This refers to when quantum computing advances to the point that it can break encryption methods. Data that is currently protected will suddenly become vulnerable.

Safeguards that would take a classical computer millions of years to decrypt will be unlocked in minutes. Q Day threatens to expose the most common public-key cryptography (PKC) algorithms such as RSA and Diffie Hellman. Entire security postures will be undone overnight.

Q Day is sometimes compared to the Millennium Bug, but there's one key difference. The Y2K bug was a computer glitch that people feared would cause widespread disruption on January 1st 2000. It was a race against the clock to mitigate the risk. It cost companies years of effort and billions of pounds[11] The potential for disruption at scale has led to comparisons between Q Day and the Millennium Bug. The main difference? No one knows when Q Day will happen.

The danger is that the lack of a date will lead to inertia. There's a risk that organisations will not grasp the urgency and fail to act now before it's too late.



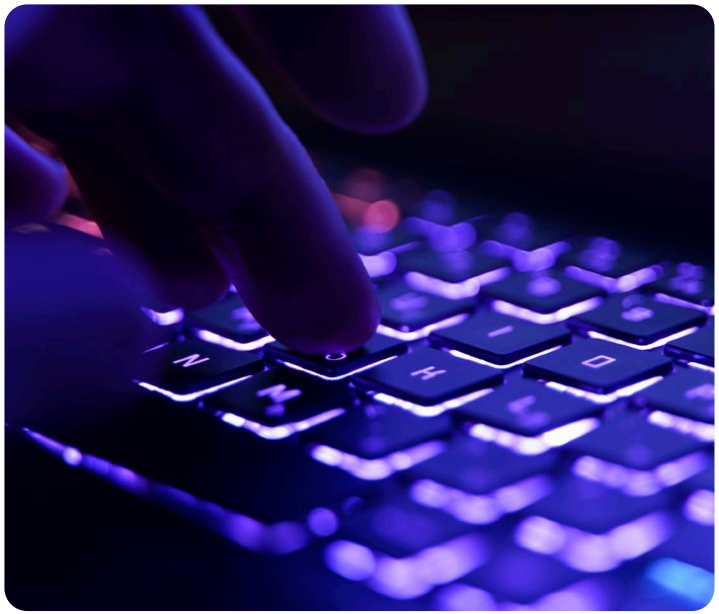
The clock is ticking

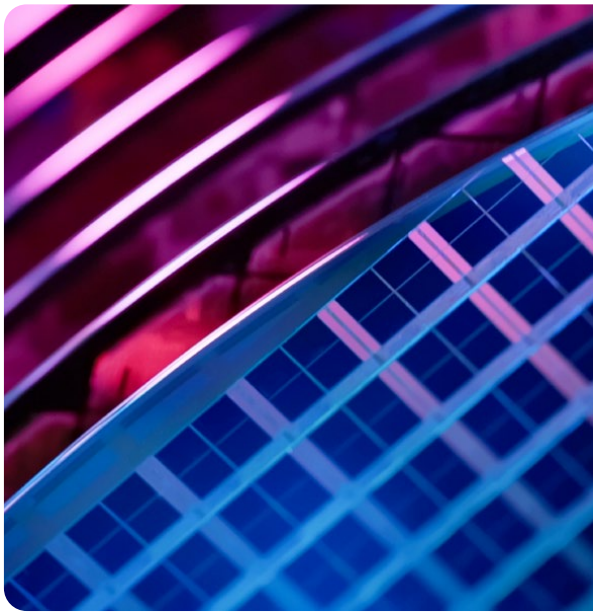
Quantum is not a future issue. Leaders need to outpace the bad actors taking action now.

This is an urgent issue for public sector organisations. Their sensitive data makes them a target. Bad actors are using a method called 'harvest now,' decrypt later,' to exploit this security weakness. They're stealing encrypted data ready for when they have access to the technology to decrypt it.

The National Cyber Security Centre flags this as a threat for organisations with high-value information.[12] Any organisation with critical infrastructure needs to act now.[13] According to the BBC, data that will still be sensitive in ten years is particularly vulnerable.[14] Confidential NHS data is therefore likely to be a prime target. Data that is harvested today could be decrypted tomorrow.

By the time Q Day arrives, it will be too late. The clock is ticking, but is your NHS organisation ready?





Quantum ready

Becoming quantum-ready is not a quick fix. The scale of work required is daunting. That's why leaders must start developing their quantum-safe strategy now.

A survey by IBM found that most organisations anticipate it will take 12 years to become fully quantum-safe. But that might not be long enough. NHS organisations must begin their journey now so they're ready when Q Day arrives.

It's all about building systems that can tackle these urgent threats while preparing for the opportunities of tomorrow. The industry is already adapting and developing post-quantum encryption standards to secure sensitive data. The level of adjustment required varies considerably. In some cases, it might just need a browser upgrade, but in others, it might require a huge transformation programme.

Leaders should be aware of the areas likely to need more work. Legacy kit may not support quantum-ready encryption. This is a major risk in a sector where many organisations rely on outdated tech. The Internet of Things and devices are also likely to be more problematic. Cybercriminals could exploit these vulnerabilities. Another potential Achilles' heel is the supply chain. NHS organisations must work with their suppliers to ensure they are developing quantum-safe strategies.

But it's not just about upgrading technology. Organisations need to be flexible enough to respond to change. This is what experts call crypto-agility – the ability to adapt quickly to new threats. Being responsive can also help with broader preparedness if the algorithm fails or there's a security breach. Nimble organisations can turn a potential threat into an opportunity.

From Ideas to Action

So how can NHS organisations make quantum-safe a reality? It starts with raising awareness and commitment at a board level to develop a robust strategy. Getting visibility of your data should be a top priority to ensure a controlled transition. It's essential to have a tight grasp of your data – where it is, where it moves and what might be relevant and open to exploitation in the future.

Secure your data with expert help

IBM Platinum Partner

Looking for expert help to navigate your quantum-safe journey? Celerity and IBM have teamed up to help NHS organisations secure their data. They'll help you develop your Data Security Strategy to protect patient safety and give you peace of mind.

Strengthen your security and prepare for Q Day with the help of industry-leading solutions. The IBM Guardium Data Security Centre helps you to:

Secure total oversight
Get complete visibility of sensitive patient data so you can understand and manage risk.

Satisfy governance requirements
A solution that ticks all information governance boxes.

Outpace bad actors
Keep up with an evolving threat landscape with near real-time early risk detection.

Proactive data protection
Enforce access policies, encryption and automated remediation.

Stop threats in their tracks
Leverage AI-powered analytics to detect and respond.

Take back control
Get peace of mind with secure access control and zero trust as an architectural principle as standard.

Use Case: Simplifying Security

IBM Platinum Partner

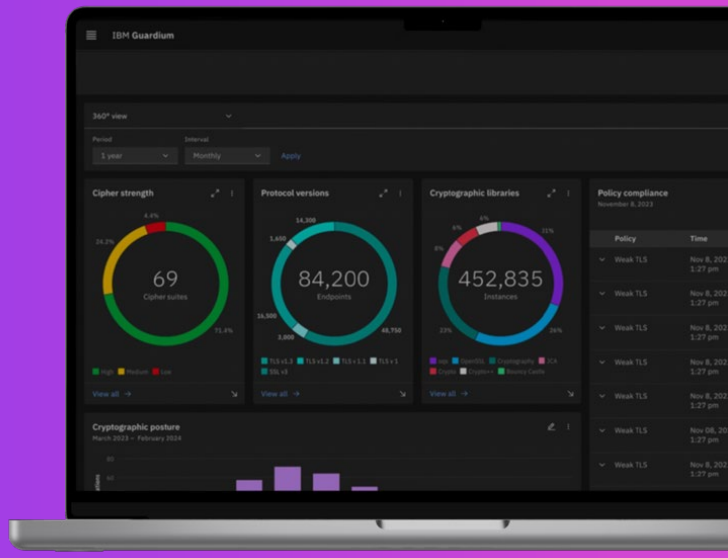
IBM helped a US-based health insurance provider to get total visibility of their data with an all-in-one solution to strengthen security and satisfy compliance requirements. The organisation made a smooth transition from their legacy system to IBM Guardium.

Before the move, the organisation was struggling with slow response times and a complex system that made it difficult to get oversight of data. They urgently needed to find an alternative option for monitoring cloud data and improving compliance with their current solution nearing end of life.

The organisation engaged with IBM to explore their options. Based on their pain points, they decided to transition to the SaaS version of Guardium Insights. This approach to platformising their data helped create one pane of glass for all security and compliance use cases.

Anticipated benefits:

- Support cloud data sources currently being supported by the previous solution
- Simplified deployment and architecture
- Less management overhead, less required resources
- Consolidated platform for all data security use cases
- Achieve 100% HIPAA and SOX compliance



Become quantum-ready

Take your first step towards proactive security. Book your discovery call to discuss your Data Security Strategy with experts so you can become quantum-ready.

Assess your security posture, uncover vulnerabilities, and build a compliance-ready strategy with expert help.

Get in touch
marketing@celerity-uk.com

Today, not Tomorrow

The quantum revolution is not tomorrow's problem - it's today's imperative. With 'harvest now, decrypt later' tactics already targeting NHS data, waiting for Q-Day means acting too late. Organisations projecting 12-year timelines for quantum-readiness will be caught off guard by a breakthrough. Even if your organisation isn't ready, bad actors will be.

Without a dedicated NHS quantum strategy, patient data remains vulnerable. This isn't merely an IT challenge but a strategic risk requiring immediate board-level ownership. As the NHS drives transformation from hospital to community, treatment to prevention, and analogue to digital, leaders must not lose sight of quantum security.

Organisations must prioritise data visibility and crypto-agility to create quantum-safe environments. By acting decisively now, the NHS can safeguard patient information and position itself to harness quantum's transformative potential for healthcare delivery. The quantum future is inevitable. Readiness is a choice leaders make today.

References

1. **BBC.co.uk. "Google unveils 'mind-boggling' quantum computing chip."**
www.bbc.co.uk/news/articles/c791ng0zvl3o

2. **BBC.co.uk. "Amazon joins quantum race."**
www.bbc.co.uk/news/articles/cly331r4p48o

3. **BBC.co.uk. "Will quantum computers disrupt critical infrastructure?"**
www.bbc.co.uk/news/articles/cpq9zxxn72qo

4. **Pulse. "Streeting sets out three NHS shifts."**
www.pulsetoday.co.uk/news/politics/streeting-sets-out-three-nhs-shifts-ahead-of-darzi-review-publication/

5. **Keir Starmer unveils Labour's mission to create an NHS fit for the future**
labour.org.uk/updates/press-releases/keir-starmer-unveils-labours-mission-to-create-an-nhs-fit-for-the-future/

6. **Gov.uk. "Lord Darzi Report."**
www.gov.uk/government/publications/independent-investigation-of-the-nhs-in-england/summary-letter-from-lord-darzi-to-the-secretary-of-state-for-health-and-social-care#conclusion-the-nhs-is-in-critical-condition-but-its-vital-signs-are-strong

7. **Gov.uk. "Data Saves Lives."**
www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data/data-saves-lives-reshaping-health-and-social-care-with-data#ministerial-foreword

8. **Gov.uk. "Cyber Security Strategy."**
www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030

9. **Gov.uk. "121 million boost for quantum technology."**
www.gov.uk/government/news/121-million-boost-for-quantum-technology-set-to-tackle-fraud-prevent-money-laundering-and-drive-growth

10. **Birmingham.ac.uk. "New hub focusing on quantum."**
www.birmingham.ac.uk/news/2024/new-hub-focussing-on-quantum-sensing-imaging-and-timing-to-be-launched-as-part-of-160m-investment

11. **The Guardian. "Millennium Bug Face Fears."**
www.theguardian.com/commentisfree/2019/dec/31/millennium-bug-face-fears-y2k-it-systems

12. **National Cyber Security Centre. "Next steps preparing for post-quantum cryptography."**
www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

13. **The Guardian. "UK Cybersecurity agency quantum hackers."**
www.theguardian.com/technology/2025/mar/20/uk-cybersecurity-agency-quantum-hackers

14. **BBC.co.uk. "Will quantum computers disrupt critical infrastructure?"**
www.bbc.co.uk/news/articles/cpq9zxxn72qo

celerity | IBM Platinum Partner | GOV.NEWS

About Celerity

Founded in 2002, Celerity initially made its name as a successful enterprise infrastructure provider before expanding into the cloud and managed services arena. The company has seen sustained growth, with UK and global coverage catering to customers across all industry sectors. Celerity people aren't just accredited technical experts with over 20 years' experience. They also care deeply, individually and collectively, about your success.

About IBM

IBM is an American multinational with a presence in 175 countries. Founded in 1911, it brings over 100 years of experience in innovation. It integrates technology and expertise, providing infrastructure, software and consulting services for clients as they pursue the digital transformation of the world's mission-critical businesses. It's about creators, partners and clients putting technology to work in the real world. Their mission isn't just to make business work better, but to make the world work better.

About GovNews

GovNews specialise in facilitating innovative and engaging partnerships between the private and public sector. We have evolved to form a leading Public Sector news brand that is well established, trustworthy and identifiable for bringing positive news, views and insights that can deliver meaningful and long-lasting change.

Our content work embodies the transition and balance from conventional engagement, like corporate strategies, thought leadership and whitepapers, to the digital realm of video, social media, and online content. We supplement this work with both online and in-person engagements and events, integrating our long and well-established expertise in event production and UK Public Sector insights.

Our latest innovation, GovNews Community, is a unique platform exclusively designed for UK Public Sector professionals. This dynamic network offers a space where members can engage in discussions, access insightful content, watch informative videos, and actively participate in a thriving community. Much like a specialised social media platform, this hub facilitates seamless interaction, enabling members to connect, share ideas, and stay updated on industry trends. By fostering this online community, we empower UK Public Servants to collaborate, learn, and exchange knowledge, creating a vibrant and supportive environment that enhances their expertise and impact within the sector.

@CelerityLimited
+44 (0)845 565 2097
marketing@celerity-uk.com
www.celerity-uk.com