

# CGI Cyber Security services for the health and care sector



## Helping the NHS and health and care providers improve their cyber security

CGI is a trusted partner of health, care and other public sector organisations across the UK, helping them achieve cyber security resilience. Health and care organisations can reduce security risks and vulnerabilities by adopting and measuring compliance with security standards, implementing good security practice and identifying strategic cyber goals, with clear ownership and responsibility established across all stakeholders.

Patients and citizens need assurance their personal data are protected and interactions with their health and care providers are safe and secure. With increasing reports of cyber-attacks, Chief Executives recognise that hard-earned trust can vanish with a single incident.

Health and care organisations are under pressure to achieve **Cyber Essentials Plus (CE+) compliance**. The first recommendation from the NHS England, NHS Improvement and Department of Health and Social Care report “*Lessons learned review of the WannaCry Ransomware Cyber Attack*” (Feb 2018) is “All NHS organisations are to develop local action plans to achieve compliance with the CE+ standard by June 2021”. However, as a result of the COVID-19 pandemic and the operational pressures across the healthcare sector, the date for certification was extended to March 2022.

### What you need to know

CE+ has five key security controls:

- **Access control** – managing effective access to authorised users
- **Secure configuration** – minimise vulnerability of computers and network devices
- **Firewalls** – properly set up to prevent unauthorised access
- **Patch management** – updates to software and operating systems
- **Malware** – protection of computers with anti-malware software

CE+ can help minimise the risk of a data breach and demonstrate that organisations prioritise cyber security. We help organisations of



### Keeping you safe

At CGI Cyber Security is part of everything we do, so although it may seem difficult to consider security while trying to innovate and extend Local Authority operations, we can help make this a reality.

We understand that Local Authorities need to protect citizen data and front-line services in order to deliver them securely. Our Cyber security services operate in three integrated areas:

- Assess the risk
- Protect the business
- Operate with confidence



all sizes to achieve relevant certifications while integrating security good practice guidelines such as the Security Policy Framework to ensure compliance with appropriate security and privacy regulations. It is vital for health and care providers to concentrate on implementing a cyber strategy. Cyber criminals will exploit any vulnerability to gain access to information networks, which can result in unmitigated access to patient records and valuable healthcare data. Cyber security incidents, resulting in breaches of data are on the increase.

Advice and guidance is available from the likes of the National Cyber Security Centre and the Information Commissioner's Office, but there are no clear standards or best practice guidelines for the health and care sector in England and Wales. This makes it difficult to recognise security and privacy requirements and achieve certification, especially during the pandemic when some health and care staff have worked from home, and needed to be "cyber secure".

### **We integrate services across the security spectrum to reduce overall risk**

Staff may not fully understand their own cyber responsibilities and the consequences of their actions if they do not follow policy and guidelines. Implications of a data breach are far-reaching, leading not only to monetary fines, but loss of public trust. We can work with you to provide focused training, guidance, services and tools to inform, educate and maintain security awareness, offering proactive Operational Security Monitoring services to identify and help resolve cyber-attacks quickly, sometimes before they happen.

Within UK Government, we have used security-specific robotic process automation (RPA) to enable security teams to automatically detect and triage incidents so they can instantly analyse and respond to threats. Previous activities that required more than two hours triaging of cybersecurity incidents now take less than one minute, allowing critical resources to use their time and skills more effectively.

### **Putting the heart back into health and care**

CGI works with clients from across the health and care sector, and our teams live and work in the same communities as the organisations we serve. Against a backdrop of unprecedented challenges, we help our clients to transform place-based service delivery, achieve cost savings and improve outcomes for their citizens and staff, bringing the benefits of our cyber security expertise to each of our engagements

## **About CGI**

### **Insights you can act on**

### **Insights you can act on**

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 82,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally

### **For more information**

Visit [cgi.com/uk/health](https://cgi.com/uk/health)

Email us at [Enquiry.UK@cgi.com](mailto:Enquiry.UK@cgi.com)