end-to-end cyber security protecting patients, employees and organisations

Clinical information is some of the most sensitive data available. We all need to trust that it's being properly protected.

For any healthcare organisation, the costs of a cyber security breach can be high – especially if data reaches the public domain.

Effective end-to-end cyber security is essential to protect patients, employees and your organisation. You need complete trust in your devices, communications, applications, data, platforms and infrastructure.

Health organisations must ensure the confidentiality, integrity and availability of their data, systems and networks simultaneously. This introduces significant levels of risk and complexity for NHS trusts and other providers.

Trusted partner for your **Digital Journey**

end-to-end cyber security

Threats continue to grow

New cyber-risks continue to emerge, with fresh attacks on healthcare organisations. The NHS is no exception – and as the threats evolve, so must the response.

Any data leak could become rapidly out of control and damage the reputation of organisations and the privacy of individuals. Moreover, a compromise to clinical data could potentially threaten lives.

Public confidence is already being tested, as with the much-publicised leaking of nearly 800 patients' details by 56 Dean Street in 2015 which resulted in a £185,000 fine for Blackpool Teaching Hospitals NHS Foundation Trust for leaking staff data, plus the revelation that NHS-accredited health apps leak data that could be used for identity theft and fraud.

Other hostile threats are emerging.

- NHS trusts may be targets for people who disagree with changes in healthcare policy.
- Criminals may look for a financial advantage, for instance with spurious overdue invoice or other 'phishing' emails to get hold of patient email addresses.
- Hackers may even try to encrypt data and seek a ransom to decrypt it. Here in the UK, two county councils have already been subject to Ransomware attacks.
- In other countries, hospitals have been targeted, such as the costly Ransomware attack on a high-profile Hollywood facility recently and similar incidents at two German hospitals.

Complying with legislation

To keep pace, legislation is evolving. The European Union is implementing two new laws to govern data protection and cyber security.

- The EU Directive on Network and Information Security came into effect in December 2015 and requires the UK Government to identify organisations that are 'Critical National Infrastructure', including healthcare providers, who will have a duty to report any cyber incidents to the Government.
- General Data Protection Regulations are new EU standards for data protection due for enforcement in 2018. They extend the scope of EU data protection to all international organisations holding EU residents' data and apply to EU data wherever it is held. The fine for a serious breach is up to 4% of an organisation's worldwide turnover.

End-to-end cyber security is critical to meet legal requirements while also ensuring that IT systems are 100% available.

Security is a critical enabler

In an ever more connected world, cyber security is a core enabler.

Health services are turning to digital technologies to help them deliver the best care while meeting financial challenges. As providers digitise, the need to secure data, systems and networks from external and internal threats increases.

In this new digital environment, effective cyber security should enable – not constrain – innovation. Trust and compliance must be at the heart of any digital transformation programme.

Balancing the response

As the digital and regulatory landscapes shift, it's a challenge for any healthcare organisation to stay informed and prepared.

Competing priorities and severe budgetary constraints only compound the pressures. But with cyber threats evolving so quickly, approaches that were effective in the past need to be re-visited.

The traditional focus on protecting the 'perimeter' of an organisation's infrastructure is no longer enough. A more complete approach to prevention, detection and response is needed. This involves real-time monitoring by a security operations centre, with behavioural analytic tools to pinpoint data loss or unusual traffic on the network (such the transfer of large files, non-finance staff carrying out financial transactions, or auxiliary staff looking at patient records).

With effective monitoring, you can then respond to threats in real time as they happen.

Keeping you protected

For over 30 years, Atos has helped mission-critical environments stay protected in a fast-changing world.

We provide end-to-end cyber security capabilities and resources that enable our clients to assess and effectively manage risk.

We offer advice, services and security products under-pinned by practical experience and rich expertise in health and other sectors. While we're often only part of our clients' overall security response, we stay committed to advising and assisting them to achieve an integrated capability.

protecting patients, employees and organisations

How we will help

Atos will help you protect against cyber threats and stay compliant with your requirements for privacy, data protection and IT governance.

We can work with you to review your current cyber security protection. We can help you develop an Information Security Strategy to identify the right security controls and real-time monitoring to prevent attacks, respond to events as they happen, then expedite any remedial action needed.

- **Assessing your vulnerabilities.** Our team of cyber security experts will work with you to identify areas of vulnerability, then assess the associated risks and how these should be managed within your wider digital transformation.
- **In-built, pre-emptive security measures and monitoring.** We will help you stay protected even as the risks evolve, and neutralise threats as they occur.
- **Supporting NHS Information Governance (IG).** Our experienced consultants will support your IG Toolkit submission, interpreting, identifying, collating, assessing and presenting evidence – including an improvement plan. This will provide assurance to your Senior Information Risk Owner and Caldicott Guardian that your IG Toolkit is a true reflection of your Information Governance Profile.
- **Improving your organisation's awareness.** We can guide you to build on your existing compliance to not just maintain, but improve your organisation's Information Governance Awareness and embed the principles into daily activity. We can also help with cyber training and awareness.
- **Reviewing your readiness.** We can review any risks to your business continuity, and carry out crisis management and cyber attack simulations to help you focus your resources.
- **Telephone advice and support,** with access to over 50 Information Security specialists.
- **Cyber security 'As-a-Service'.** For organisations making the move to the cloud, we provide cyber security capability, monitoring and response are included as part of cloud services.

We understand your competing pressures. That's why we'll tailor our approach according to what you need. One good place to start is to carry out a Cyber Security Health Assessment to assess your current level of risk and where resources should be targeted – especially within tight financial constraints.

Our experience

Atos brings an unparalleled combination of:

- extensive **security expertise in Government-regulated environments;** we have provided security advice and services to most UK Government Departments including the Ministry of Justice, Department for Work and Pensions and Home Office
- specialist **health sector security experience:** we are a major IT outsourcing provider for NHSScotland, protecting clinical data from unauthorised access or disclosure from cyber attacks
- detailed, practical experience of the **NHS Information Governance (IG) Toolkit.**

Summary

While cyber security threats are growing, the impacts of a security breach for healthcare organisations could be significant. In response, the regulatory environment is getting tougher with the likelihood of mandatory breach reporting and greater financial sanctions for non-compliance.

You need cost-effective cyber-security solutions that protect against evolving threats while reducing the barriers to people accessing the tools and data they need.

At Atos, we understand the challenges of safeguarding health information in an increasingly connected, complex digital environment.

We work with Trusts and other organisations to identify areas of vulnerability, assess the associated risks and how these should be managed within a trust and compliance framework.

For more information about how cyber security issues are affecting UK Health please visit uk.atos.net

About Atos

Atos SE (Societas Europaea) is a leader in digital services with pro forma annual revenue of circa € 12 billion and circa 100,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.