CASE STUDY

Securing Patient Data and Achieving ISO 27001 Certification

NHS
King's College Hospital
NHS Foundation Trust

Overview

King's College Hospital NHS Foundation Trust, managing several major teaching hospitals in London, engaged i3Secure to certify to ISO 27001.

The ICT Department, which manages the complex ICT framework across the Trust, had long aspired to attain ISO 27001 certification, an international standard for information security. Alongside their existing well-established technical controls, this goal showed commitment to ensuring a robust, secure digital environment for the Trust.

A challenge in the public sector is retaining specialist talent, especially in cyber security. Recognising the necessity for ISO 27001 expertise, the Trust sought a proficient partner to help them achieve ISO 27001. With a strong reputation and extensive experience, i3Secure was chosen as the Trust's partner.

The Challenge

There were two key challenges to overcome for the Trust to achieve ISO 27001 certification.

Firstly, maintaining rigorous information security in a large hospital can be challenging, especially when patient care is the priority. Clinicians and other staff focused on delivering high-quality patient care may not always prioritise adherence to stringent information security protocols if perceived as hindering their primary duties.

For such a complex organisation, it was thus crucial for our Consultant and the ICT team to ensure the scope of the certification aligned with the Trust's operational realities. This would give them the best possible chance of successful implementation and compliance.

Secondly, as a public, non-profit body, a primary hurdle was managing the constraints of budget, resources, and skill availability. At the time of our Consultant's arrival, the Head of Cyber Security role was vacant. This posed a challenge due to the difficulty and expense involved in filling such a specialised role permanently. This vacancy necessitated a temporary redistribution of responsibilities among the existing ICT department members, who were juggling their regular duties with the added demands of overseeing cyber security tasks.

i3Secure offered the Trust industry-leading expertise at comparatively low cost, fitting seamlessly into the organisation to fill the skills gap.

© 2023 i3Secure Ltd

Our Solution

Our Consultant built an Information Security Management System (ISMS) that would serve the ICT department in their operations and aid assurance of the security of its information.

Given its size and complexity, it was recognised that aiming for ISO 27001 certification for the entire Trust might not yield the most efficient or cost-effective results. Thus, it was strategically decided to first focus certification efforts on the ICT department. The scope would then be extended to include other departments and the wider Trust in future phases, ensuring controlled, effective implementation.

Our Consultant conducted systematic internal audits throughout implementation, meticulously covering all the standard's requirements. The audit findings were regularly reported back to management, keeping leadership informed on progress.

i3Secure improved the Trust's documented governance, addressing gaps that could lead to non-conformances during external audits. Improvements included a new classification scheme tailored to the department's needs, new procedures for identifying and addressing security events, and new information security and data privacy policies. These measures were swiftly adopted and improved compliance and audit readiness.

Our Consultant attended all eight days of the audit, guiding the auditor through the new ISMS. The audit coincided with launch of new electronic patient record system Epic, meaning ICT staff were exceptionally busy supporting clinicians. The Consultant's expertise minimised effort required from ICT staff, allowing them to focus on supporting frontline staff and prioritising patient health. This was vital in navigating the audit with minimal disruption to healthcare services.

The Result

The Trust achieved the distinguished status of being among the few hospital trusts certified to ISO 27001.

This garnered significant recognition from London's Integrated Care Board and NHS England. Both have expressed interest in using the Trust as a model for other NHS entities to emulate, viewing the Trust's journey to ISO 27001 certification as an exemplary case study in enhancing information security standards.

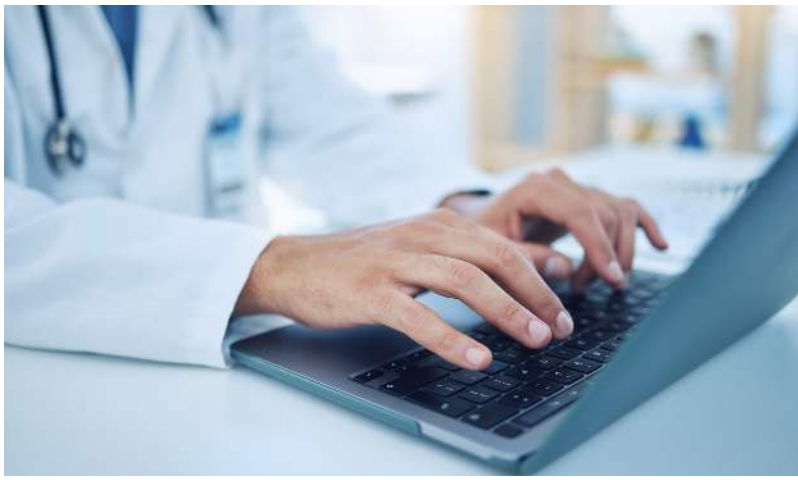
i3Secure's work with the Trust's ICT staff to develop their ISMS has enhanced its capability to manage information effectively and safeguard patient data. This has had a far-reaching impact, as it now underpins cyber and information security across the entire Trust.

This project highlights i3Secure's commitment to delivering secure and efficient data management solutions, reinforcing the safety and integrity of patient information across the health sector.

Our Client's Words

"We found i3Secure responsive and capable in providing the support we needed as the ICT department achieved ISO 27001 certification. The Consultant was professional in delivering the work needed to get us to the right level and was unflinchingly focussed when it came to getting done on time what was necessary."

Head of ICT Service Management



© 2023 i3Secure Ltd