CASE STUDY

King's College Hospital NHS Foundation Trust

Securing Patient Data and Achieving ISO 27001 Certification

Overview

King's College Hospital NHS Trust, which manages several of London's largest teaching hospitals, engaged i3Secure to assist in implementing the ISO 27001 standard.

The Information and Communication Technology (ICT) Department had long aspired to attain the ISO 27001 standard, an international benchmark for information security. Recognising that their technical controls were already well implemented, and their goal to achieve ISO 27001, showed their commitment to ensuring a robust and secure digital environment for the Trust.

Operating from one of their London hospitals, the ICT Department is responsible for managing the comprehensive ICT framework across the Trust. This role is particularly crucial in an era where healthcare management is transitioning from traditional paper records to digital platforms, significantly increasing the scope and importance of their work.

One of the most significant challenges in the public sector is retaining specialist talent, especially in cyber security. Consequently, recognising the necessity for ISO 27001 expertise, the Trust sought a proficient partner that would help them achieve ISO 27001. With an excellent reputation in the health sector and extensive experience assisting various healthcare organisations, i3Secure was chosen as the cyber security partner to help the Trust achieve ISO 27001 certification.

The Challenge

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

Firstly, in a large hospital setting, maintaining rigorous information security can be challenging, especially when patient care is the utmost priority. Clinicians and other hospital staff, primarily focused on delivering the highest quality of patient care, may not always prioritise adherence to stringent information security protocols if they perceive these as hindering their primary duties.

Consequently, for a complex organisation like this, it was crucial for our Consultant and the ICT team to consider the scope of the ISO 27001 certification and ensure it aligned with the Trust's operational realities, and they had the best chance of successful implementation and compliance.

Secondly, as a public, non-profit body, one of the primary hurdles for the team was managing the constraints of budget, resources, and skill availability. At the time of our Consultant's arrival, the role of Head of Cyber Security was vacant, posing a significant challenge due to the difficulty and expense involved in filling such a specialised role on a permanent basis. 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 were able to offer the Trust industry-leading expertise at comparatively low cost and fit seamlessly into the organisation to fill the skills gap.

Our Solution

Our Consultant worked under the management of the Deputy Director of ICT and alongside the Head of ICT Service Management to build an Information Security Management System (ISMS) that would serve the ICT department in their operations and support the assurance of the security of its information.

Early in the process, it became clear that aiming for ISO 27001 certification for the entire Trust, given its size and complexity, might not yield the most efficient or cost-effective results. Such an approach risked inefficiency and unnecessary costs. Therefore, it was strategically decided to first focus the certification efforts on the ICT department. Following the successful certification of the ICT department, the scope would extend to include other departments, eventually encompassing the entire hospital and the wider Trust in future phases. This phased approach ensured a controlled and effective implementation of the certification standard.

Our Consultant planned and executed systematic internal audits throughout the duration of the implementation and meticulously covered all aspects of the standard's requirements. The findings from these audits were regularly reported back to management which ensured that leadership stayed well-informed about the ongoing progress and understood the necessary steps ahead.

i3Secure played a pivotal role in enhancing the Trust's approach to documented governance, which, despite the department's comprehensive technical controls and sound management, faced challenges due to its complexity. Recognising that this gap could lead to non-conformances during external audit, our Consultant took measures to address this. A newly designed classification scheme was one element, tailored specifically for the department's needs whilst being cognisant of the wider organisation. A second element was implementing new procedures for identifying and addressing security events and vulnerabilities. A third example of improvements in this area were the new overarching policies we introduced for information security and data privacy. These new additions were swiftly adopted, significantly improving the department's compliance with security protocols and readiness for external audit.

The Result

The Trust has achieved the distinguished status of being among the select few hospital trusts certified to ISO 27001. This accomplishment has garnered significant recognition from London's Integrated Care Board and NHS England, both of which have expressed interest in using the Trust as a model for other NHS entities. They see the Trust's journey to ISO 27001 certification as an exemplary case study, offering valuable insights and practices for the wider NHS to emulate in their pursuit of enhanced information security standards.

i3Secure's collaboration with the Trust's ICT Department in developing their new Information Security Management System (ISMS) has been a significant project. The measures taken to achieve ISO 27001 certification were pivotal in enhancing the organisation's capability to manage information effectively within their department. More importantly, this has had a far-reaching impact on the entire Trust, as the ISMS now stands as the backbone of cyber and information security across the organisation.

Being a trusted partner to a number of NHS organisations, i3Secure's engagement with the Trust has provided them with the assurance they need for safeguarding patient data. This collaboration highlights i3Secure's commitment to delivering secure and efficient data management solutions, reinforcing the safety and integrity of patient information across the healthcare sector.

"Throughout our engagement with i3Secure on our journey to ISO 27001, they have all been professional, helpful and willing to ensure that we reached the standard required.

Leading on their behalf was their Consultant, who proved to be invaluable in guiding us through the process. His patience with our NHS processes and delays was appreciated while his attention to detail meant that we achieved certification with no major findings. His depth of knowledge on the ISO 27001 and the processes for accreditation ensured that we stayed on track throughout the journey. The Consultant's gentle humour and infinite flexibility made it a pleasure to work with him. We look forward to continuing to work with i3Secure over the coming years to retain our certification."

Deputy Director of ICT