What's next

Healthcare

Five steps toward NHS cyber security compliance

There are a bewildering number of guidelines and rules when it comes to meeting NHS cyber security, safety, privacy and risk management for any organisation working in the UK healthcare sector. For example, the documentation alone required to set up as a software vendor to the NHS can be daunting. Depending on the size of your company and the resources available to you, some of these certifications may seem too complex to put in place. However, if you take them one at a time, getting the right certifications is important and will pay off in the long run. Here are my top five tips for healthcare software providers:

Ian McGuire

Posted 28 May 2019

1. Start as you mean to go on

Make sure you have clear company policy documents covering staff and employment practice, and that you can prove that the policies are working – this gets more important as you ascend the heights of Information Governance (IG) compliance.

2. Get the basics right

Register with the Information Commissioners Office where there is lots of information helping you get your **GDPR** and Data Processing agreements and policies in place. It is important to conduct Privacy Impact Assessments for your software externally and your processes internally. Make sure your staff are regularly trained on Information Governance and you can prove it. Also make sure you are registered on the Organisation Data Service with your primary contracting entity. It is also a good idea to sign up for Cyber Essentials (Plus)

3. Make sure you comply with DCB0129

This lesser known guideline kicks in when you start processing patient data, or you are involved in decision support or telehealth. This involves performing Clinical Risk Management on all changes and new features in your software. It is a development task resulting in a Safety Case document showing the risk analysis before and after changes and should be

released in line with your regular release notes.

4. Comply with Data Security and Protection Toolkit

Complying a data security and protection toolkit is a more involved process and one which starts you on the road to having ISO27001. This online questionnaire requires you to evidence all processes and procedures relating to Data Security and protection. If you have done the above properly then you should have these processes in place such as internal governance policies, staff contracts and training and physical and cyber security. Most NHS Trusts will require this as the basic standard for working with patient data.

5. Meet ISO27001

This usually satisfies most security related queried from the NHS. Depending on how organised you have been in the previous sections this could be a relatively simple certification. Alternatively, it can be a time consuming task if you are a large, disparate organisation. Scope here is everything – define this well and save lots of time. In my experience it is easier for smaller companies to achieve this if they have the processes in place already and it is economically viable. This is especially relevant if you are hosting a solution into the NHS or if you provide services from abroad. You must be externally certified for all related processes and IG policies as well as security management systems, physical security, business continuity, incident reporting and so on. My advice is to create a definitive security document encompassing all the certifications here for each client. They will never doubt your security again.

Tags: Information Governance, Risk Management

More Information

About Ian McGuire

Ian McGuire is an industry expert in voice biometrics, speech recognition, and customer experience design. He is Senior Principal Business Consultant in Nuance and provides consultancy to large organisations across the financial, telecoms and government sectors, on the introduction of new and innovative technologies that will materially impact customer experience and business processes. Ian worked with all the major UK banks, as well as a number of European and Hong Kong banks, in deploying counter fraud and voice biometric authentication solutions. Also with major credit card organisations, wealth organisations and telecom companies to deploy customer ID&V solutions, and online and offline fraud detection systems.

View all posts by Ian McGuire