What's next

Healthcare

How do Dragon Medical solutions adhere to the data security standards outlined within GDPR and regulations set by the NHS?

Data security in healthcare has always been of paramount importance with the need for patient data protection and confidentiality being a significant concern for all organisations. Now, with the recent introduction of GDPR, and a number of high-profile cyber-attacks on NHS infrastructure, many are taking an even closer look at data protection and computer system security issues.

Sarah Fisher

Posted 17 August 2018

The new NHS data security requirements

The ‘2017/18 Data Security and Protection Requirements’ set out what is expected of NHS organisations and those working with the NHS, in meeting the ten data security standards established. This document breaks the requirements down into three key areas: people, processes and technology. Included within the latter is the requirement to ‘identify unsupported systems (including software, hardware and applications) and… remove, replace or actively mitigate the risks associated with unsupported systems.”

It also requires that all IT suppliers and software have relevant certification, and states that all organisations working within and for the NHS must carry out on-site cyber and data security assessments if asked to do so by NHS Digital. This means that it’s essential that you are confident that the software you are using is secure and robust enough to protect patient data.

Protecting the digital future of healthcare

Aside from the current organisational requirements for secure healthcare communications, it can also be seen as the role of all who work in the healthcare sector to protect the sensitive data of all patients. As health organisations increasingly rely on digital technologies – often exclusively – to handle patient documentation and other tasks, the efficiency and flexibility of the service is increasing, but so too are the risks.

According to a survey by Digital Health, more than 50% of NHS acute trusts have electronic patient record systems, reflecting the shift towards technological solutions. The ‘WannaCry’ cyber attack of 2017 meanwhile – which affected more than a third of trusts in England – served as a wake-up call highlighting the vulnerabilities of a modernising healthcare system. Though no patient data was compromised in the attack, a report by the National Audit Office found that it could have been prevented if NHS trusts had acted on ‘critical alerts from NHS Digital’, regarding updating or replacing older software.

A breach of security can result in grave consequences, such as the loss of patient data and other protected health information, organisational penalties and decreased confidence in the healthcare system. For NHS suppliers, it may even mean the loss of vital contracts. Taking pre-emptive action to ensure that patient data security measures are robust is therefore vital.

How Dragon Medical solutions can protect your patient data

Dragon Medical One is built to suit the current security demands of the NHS and the wider healthcare sector, as all speech-to-text patient data is communicated securely via 256-bit encryption channels. This robust transfer method is bolstered further by the use of Transport Layer Security (TLS) protocols compatible with all popular EPR platforms, including Allscripts, Cerner, Epic, EMIS and Meditech.

GDPR requires that personal data is processed securely by using, ‘appropriate technical and organisation measures’. This means using software which is inherently secure. All of Dragon Medical One’s cloud services are protected by Microsoft Azure’s data centre security, and Nuance follows all IT security best practices to ensure the integrity of customer data. The software is also engineered with security at the forefront, utilising Secure Software Development Lifecycle Techniques and Veracode static code analysis.

Nuance’s software connects directly and securely to NHS England’s N3 national broadband network. This means that physicians can record directly into the patient record, and share any relevant files with other departments and Trusts across NHS England’s dedicated secure cloud network.

Long-lasting solutions for healthcare data security

Data security in healthcare is an issue that is going to grow over time, and the only way to deal with it is to ensure that your organisation and its processes are properly protected. Dragon Medical One and Dragon Medical Practice Edition can help you to ensure not just that your organisation is efficient, but that you’re on top of patient data protection requirements.

Find out more about Dragon Medical solutions today.

Tags: data security, GDPR, health IT, Patient data

More Information

Data Security in Healthcare

Discover how Dragon Medical solutions meet the standards of patient data security set in the UK

Learn more

About Sarah Fisher

Sarah Fisher is regional marketing manager at Nuance healthcare division covering UK, Ireland and APAC. Sarah has 25 years in marketing and sales at companies including Xerox, Siemens and Cisco. A spell at Novartis leading a team to deliver ‘more-than-medicines’ solutions in UK healthcare combined her degree and a first job in Pharmacology research with a passion for the potential of healthcare IT to overcome the many challenges faced by all healthcare systems. In her spare time Sarah leaps fences and tackles tricky trails pursuing her hobbies of horse trials and mountain biking.

View all posts by Sarah Fisher