Security and the Digital Future of the NHS

Delivering digital solutions and services that are optimised for clinicians’ workflow needs and secure for NHS organisations.
“Clinical staff want very quick access to everything, wherever they are. Their user experience was key to any new system we developed.”

Jonathan Murden | IT Operations Manager | Portsmouth Hospitals NHS Trust

The NHS is currently evolving to meet the needs of an ageing population. This means that not only is the delivery of clinical care more challenging in the acute hospital setting but it increasingly relies on enhanced information access in the primary care, mental health and community environments too.

The Five Year Forward View (FYFV) made it clear that integrated care models are the future of the NHS and this will clearly depend on technology as an enabler. However, associated with greater investments in digital systems are increased information threats which healthcare organisations need support to manage at an end-user level while also complying with developing regulatory guidelines.

Empowering Clinicians

One of the key components of the future success of the NHS is its ability to digitise its workflows. As with any complex project there have been shifting timelines as to when a paperless or paper light state can be achieved with a provisional target year of 2023 being recommended in the recent Wachter Review commissioned by NHS England. Despite this, trusts, particularly in the acute setting, have invested significant sums in the adoption of outright electronic health record (EHR) solutions (e.g. Cerner, Allscripts, Epic etc.) or invested in a ‘best of breed’ strategy to deliver an EHR experience for their clinical workforce. However, investing in technology is only one part of the jigsaw puzzle of evolving the NHS to continue to deliver high standards of clinical care whilst being increasingly efficient. Technology enabled change is still universally dependent on the positive engagement of clinical end-users.
The recently released Wachter Review underscored the importance of the roles that clinicians will play in the digital evolution of the NHS at both local and national levels. In line with this, a national Chief Clinical Information Officer (CCIO) was recently appointed within NHS England demonstrating clear commitment to clinical engagement. Therefore, any discussion about security and information governance must take into consideration the needs of clinicians. Particular factors include:

- The variability of workflows based on roles
- The variability of their workflows depending on settings (e.g. Clinic setting vs. Emergency department)
- The variability of workflows based on roles
- The volume of communication and information sharing required between clinicians to manage their patients
- The number of applications they need to access to complete a full patient history
- The level of mobility they require both inside and outside a hospital for patient management
- The increasing dependence on personal mobile devices

With these factors in mind it is crucial that the introduction of new applications does not disrupt and hamper existing workflows but instead offers a smooth transition.

The objective of a clinician is to care for their patient in a timely and effective manner. If an application obstructs this then clinical staff will employ workarounds. This can include using personal applications to communicate patient data with other clinicians or sharing credentials in order to access necessary clinical applications. These are all sources of information governance risks but are happening because clinical staff feel restricted within their workflows. These risks are increasingly being recognised by regulatory bodies and so trusts face a challenge balancing security requirements with workflow needs.

### Evolving Regulatory Guidance

Recently, both the Care Quality Commission (CQC) and Dame Fiona Caldicott discussed in detail the importance of cybersecurity and information governance standards within the framework of a digital NHS.

The reason for this renewed focus is in part because of anecdotal evidence reported at local levels of inconsistent information management practice but also because formal reporting from the Information Commissioner’s Office (ICO) continues to place healthcare as one of the most profound sources of data breaches. In the year 2014/15, the ICO reported that as a proportion of reported data breaches the health sector accounted for approximately 45%. Meanwhile, between January and March 2016 over 150 data security incidents had been reported to the ICO which was three times the number as any other industry. Although the majority of breaches are still considered to be due to misplaced paper records containing patient information or lost devices, there is undoubtedly a recognition that an increasingly digital environment presents its own data security challenges.

In Dame Fiona Caldicott’s latest report (Caldicott 3) a number of sources of risk were identified such as the presence of outdated or unsupported IT applications being present within trust IT ecosystems. However, there was also the acknowledgement that poor user design or the imposition of security standards that impede clinical workflows can lead to end-user workarounds being incentivised.

Taking these observations into account, it is therefore important to ensure that clinical engagement is supported as a part of the development or introduction of any data security standards at a local level and particularly when these are adjustable through the introduction of a new application or platform. Accordingly, the Care Quality Commission released their own data security review of the NHS in England in 2016. Some of their conclusions included:

- The digitisation of healthcare eliminates paper based risks but may expose institutions to larger scale risks
- Security systems are, in some cases, designed without end-users in mind
- Incidents are investigated in detail but more needs to be done to disseminate lessons learned
- Integrated care means there will be increasing data sharing and so appropriate security protocols need to be implemented

With these discussion points in mind, the CQC recommended that more needs to be done to manage data security within the NHS. Their recommendations were defined according to people, processes and technology with a security-specific training, leadership and audit processes being emphasised. To underscore their own commitment to this, the CQC stated that it would amend its assessment framework to include the aforementioned factors and would therefore train its inspectors accordingly. Associated with an amended CQC inspection framework a recommendation was also made that the ICO’s Anonymisation code should be used as the minimum safeguard standard for the NHS which acts in line with the Data Protection Act (DPA) which for serious breaches may lead to fines of up to £500,000.

Factored within all this is the prospect of the introduction of the European Union’s (EU) new General Data Protection Regulation (GDPR) which will be implemented across the EU by 25 May 2018. Despite the Brexit vote, many of the principles of GDPR are likely to be implemented to enhance patient safeguarding. However, it is worth noting that a recommendation within GDPR states that supervisory authorities should have the authority to sanction penalties for severe regulatory breaches totalling up to £20m. Although this may be considered unlikely within the NHS, it illustrates the critical importance of protecting patient data in the future.
This emphasis on security in the NHS also fits within the National Cybersecurity Strategy which was launched in November 2016 by the Chancellor of the Exchequer, Philip Hammond. As a part of this, £1.9bn has been earmarked to enhance the cyber-defense capabilities of the UK over the next five years and specific mention was made within the accompanying report of the variation in cybersecurity capabilities of the 40,000 organisations and 1.6m employees that operate within the NHS.

Clinical Risk in Practice

Although there are a number of recommendations that will be enforced over the coming years it is important to consider existing risk standards within the NHS. The most commonly referred to standard at the operational level is that governed by the Information Governance (IG) toolkit (SCCI0086) which is a mandatory annual self-assessment tool used by both NHS organisations and suppliers to assess their compliance with a range of adopted information governance standards.

There is additionally a separate set of standards that specifically identify the management of clinical risk as a part of the design and implementation of IT systems within healthcare organisations. These standards SCCI0160 and SCCI0129 are applied to providers and suppliers respectively. When taken together in practice they define a process that should be adopted that allows healthcare organisations to work with suppliers to benchmark the clinical risks associated with the implementation of IT systems and to define processes that will mitigate these risks. Interestingly, they also identify the importance of the role of a Clinical Safety Officer being appropriately trained and present both within NHS and supplier organisations to oversee compliance. Within increasingly mobile and interoperable environments, these will be essential standards to ensure that information security and governance standards are maintained to this highest possible levels while reducing the impact on clinical workflows.

Given the increasing complexity of managing the patient population, the mobile requirements of clinical end-users, looming regulatory guidelines and the increasing number of cybersecurity threats facing NHS IT systems it is critical that trusts can invest in solutions they can rely on.

How Citrix delivers security and enhances clinical workflows

Citrix solutions for healthcare IT are developed and implemented with the multifactorial needs of the NHS in mind. The foremost of which is the ability to enhance the clinical workflows of end-users. Whether organisations are reliant on fixed end-points, mobile devices or a combination of the two, there is a Citrix solution to optimise the clinical workspace. The delivery of virtualised environments and ‘follow-me’ desktops means that clinicians are able to mobilise their EHR and application environments according to their workflow needs across any device and multiple facilities. Additionally, through mobile application management, Citrix can empower trust mobile strategies regardless of whether they are based on allocated devices or a ‘bring your own device’ (BYOD) strategy. These components all serve to enhance the user experience of the overall IT application ecosystem for clinical end-users allowing them to focus their time more optimally delivering patient care rather managing their IT applications which ultimately leads to a better patient experience. However, these solutions also have market leading capabilities when securing mobile clinical workspaces and minimising risks to patient data.

Protecting Patient Data

At a technical level, there are a number of ways Citrix can protect data within the data centre in ways that are more powerful than local end-point firewalls and anti-virus platforms including through the use of:

- Next-Generation Firewalls
- Intrusion Protection Systems
- Granular Access Controls

This introduces protection against patient data loss that happens to be due to human errors arising from software and hardware failures.

However, beyond this, administrators, preferably with clinical guidance, can also manage access and provisioning of their application ecosystems to balance security against workflow requirements. Protecting patient data in an increasingly mobile environment is a challenge especially when there is an increasing tendency towards BYOD strategies. Managing data and applications residing on devices ranging from laptops to smartphones introduces a broad surface for attack or accidental breaches. Given the complexity of clinical user requirements there are also varying access control requirements depending on role, seniority and clinical context. Citrix can mitigate these challenges by delivering a solution which allows administrators to use a single toolset to manage access policies across its entire user population without being restricted to their device choices or locations.

This toolset can also be used for rapid provisioning and de-provisioning. This streamlines the ability of an organisation on-board new clinical users in a secure manner managing their precise access according to their clinical workflow requirements. Managing this through an enterprise application store also means that a trust and its end-users can be confident of the source and quality of the IT applications for patient care. This goal of this functionality is to mitigate the risk of patient data residing on a device which can be compromised while delivering an intuitive mobile, clinical application experience for a trust’s end-users.

At a broader level, these features also support organisations to meet the core technical requirements of the Cyber Essentials scheme which is a government and industry backed initiative to guide organisations to implement controls that will protect their information assets against common, low level security attacks.
Demonstrating Compliance

When investing in new IT applications and platforms, IT and governance leaders need to be confident that not only can they secure patient data but that they can also demonstrate regulatory compliance. Even if a breach occurs, there must be systems in place which can mitigate the risk and provide intelligence for the purposes of auditing and investigation. The ability to investigate and disseminate lessons learnt was a key discussion point in the CQC’s recent report. Citrix solutions contain a simplified toolset enabling the administrators to have complete, centralised auditing capabilities to identify and map when and which users accessed applications and datasets as well as track devices. This simplifies the ease of auditing for administrators as they no longer have to collect audit information from individual devices. Further features that confer security and governance compliance capabilities include:

- An integrated application container for mobile devices and applications enables:
  - Password authentication
  - Data encryption
  - Secure lock and wipe
  - Inter-app policies
  - Micro VPNs to mobile apps

These features introduce security and demonstrable compliance features for trusts implementing BYOD strategies. Administrators have full policy control of the organisational applications and data while keeping personal device data completely separate and untouched.

- Virtualised environments are completely secured within data centres due to the implementation of standards based encryption standards, multi-factor authentication and, secure remote access and event logging.

- Citrix solutions for healthcare IT include a secure enterprise file sync and share service empowering clinical end-users to share data securely rather than through insecure communication methods (e.g. e-mail) which are difficult to audit and a potential source of data breaches.

These features ensure not only a secure clinical workspace but also maximise an organisation’s ability to meet compliance standards.

Conclusion

The NHS is going through a digital transformation that will be significantly defined by the ability of clinicians to operate within increasingly mobile environments. Security and information governance vulnerabilities have been pre-emptively identified as a part of this shift in practice from paper based to digital systems and mobile workflows with clear guidance and regulations being proposed at both national and international levels. Citrix IT solutions have been developed based on the needs of end-users and in healthcare this means securely enhancing clinical workflows while optimising IT system performance. Citrix delivers virtualised desktops and applications for clinicians which are centrally configured and managed by system administrators.