AbedGraham
Healthcare Strategies

Caldicott, Clinical Risk and Health IT suppliers

A White | Paper

By Dr Saif F Abed &
Dr Gabriel K Ma

Following the recent release of the “Review of Data Security, Consent and Opt-Outs” , by Dame Fiona Caldicott, the National Data Guardian for Health and Care (NDG), this white paper explores some of the key themes raised, and highlights the key challenges and opportunities available for health IT suppliers to capitalise on. There will be a focus on a number of significant findings on Data Security that strengthen established insights at AbedGraham rather than just the common issues of consent and opt-out.

Enforcing New Data Security Standards

Following on from the NDG’ s previous Review in 2013, it was noted that there had been little positive change in the use of data across health and social care. In this third Review by the NDG, the focus was not only on identifying new standards, but also involved recommendations in precipitating real world change. This included plans to increase monitoring of compliance with these new standards, guidance about the responsibility of organisations and suppliers involved in data management and clarity of consequences around not managing data securely. Although these plans may appear to place more obligations on IT vendors, the implementation of business strategies that manage these issues effectively, can only help suppliers stand out against their competitors.

Key Challenges

Impact on IT suppliers

As an example of how IT suppliers will be under increased scrutiny, one of the recommendations explicitly stated as one of the new Data Security Standards, is the responsibility of the IT supplier to be held accountable via contracts for protecting the personal confidential data they process. With respect to their involvement regarding information governance risks, in order to help establish compliance with the new standards, recommendations have been put forward for the Care Quality Commission (CQC) to amend its inspection framework and approach, to include assurances that the appropriate validation against the new standards has been carried out.

There is also an increased focus for there to be a potential change in the financial contracts of organisations, to take account of the new data security standards, with contracts to not be extended if a provider does not meet the standards. Arrangements for data security auditing are to be reviewed and strengthened to a level similar to those assuring financial integrity and accountability.

A further recommendation of the Review to deliver real change, is the consideration for the Information Commissioner' s Office' s (ICO) Anonymisation Code to be used as the minimum standard to safeguard all de-identified data in accordance with the Data Protection Act (DPA), with penalty notices of up to £500,000 for serious breaches of the DPA in regards to deliberate and negligent re-identification.

Consequences of poor Data Security

The use of unencrypted devices resulted in a fine of £325,000 to a single NHS Trust.

Across the health sector the ICO has issued 11 fines amounting to £1.4 million between April 2010 and November 2015.

Causes of Data Breaches

When considering the factors that contribute to data breaches, three areas were identified: people, processes and technology. Breaches are often caused by individuals finding workarounds to burdensome processes and outdated technology. This demonstrates the importance of clarifying and streamlining the underlying clinical workflows and operational processes that IT solutions need to optimise.

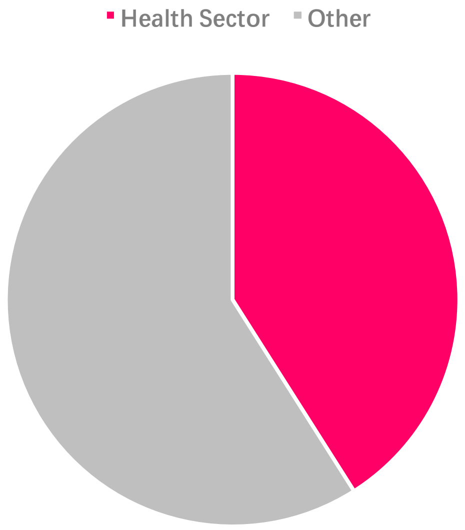

Figure 1.0 An illustration of the proportion of breaches from the health sector at the Information Commissioner' s Office 2014/2015.

Many of the information breaches historically reported by the health and social care sector related to patient information on paper, or to technologies such as faxes. Although the Review suggests that as the health and social care sector moves towards a paperless digital future, many of these issues will be addressed automatically, it would be prudent to pay attention to the delays in achieving interoperability, alongside the shift in focus to increased integrated care that may impact the delivery of this change. It is likely that there will be continued paper and fax use whilst these issues are being resolved. The involvement of Managed Print Services (MPS), for example, would still require careful attention with respect to Information Governance concerns. In addition, the advancement towards electronic working is not free from clinical and governance risks, and compliance with the new Data Security standards will still be required when sharing and sending information to various other services. Rigorous review of clinical workflows and operational processes before and after mapping to electronic working pathways are integral to minimising associated risks.

Drivers behind human behaviour

The Review heard that technology can become a source of risk when it is out of date and unsupported, and that there is significant use of software within the sector that is no longer supported by the manufacturer. This means that security fixes are no longer produced. Unsurprisingly, recommendations were made that secure and up-to-date technology is in place, both through the procurement process and the lifecycle of the technology within the organisation. There was also a mention that when processes are poorly designed or communicated, users will often revert to doing something in the most convenient way.

The balance of security against accessibility was also raised. The Review heard the suggestion that security needs to serve as an enabler, so as not to be perceived as a blocker, and that clear tension emerged between attempts to follow the security processes, and the practicalities of needing to access information. The use of multiple logins required to access several applications was reported to be time consuming, despite use of a smartcard, and access cuts out after a short period of inactivity. This again highlights the importance of understanding the clinical processes that IT are to optimise. In the scenario of access cutting out due to inactivity, there should have been close dialogue with clinicians and technical staff, to gain an understanding of the variation of access times, to be able to employ a tailored solution.

Main data Security issues in Health Q3 2015/2016

22% of incidents were Data being posted or faxed to an incorrect recipient.

20% of incidents were related to loss of theft of paperwork.

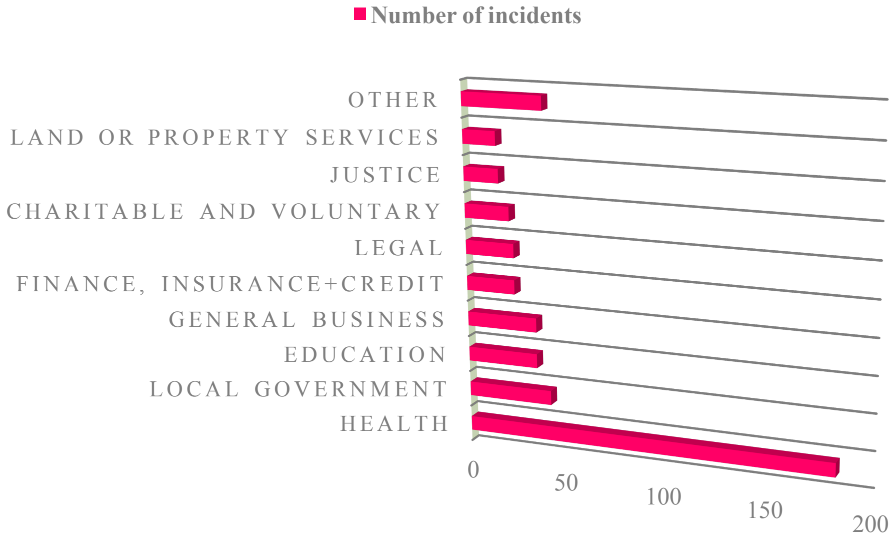

Figure 2.0 A breakdown of data security incidents across sectors Q4 of 2015/16 (January -March 2016) taken from the Information Commissioner' s office

Interesting points on Data Security

"The number of breaches is rising, although the reasons for this are unclear."

"Breaches largely happened due to human behaviour."

The National Data Guardian, 2016

Disenfranchised staff

Evidence of this disconnect between clinical and IT staff was found when the Review heard strongly that "IT security need to walk in the shoes of a clinician for a day" and poignant statements such as "the system that is supposed to support staff, doesn' t" . The most successful projects when implementing IT solutions leverage a strong working relationship between clinical and IT staff. Investing in this relationship is vital if IT projects and transformations are to be maximally efficient and in line with the new Data Security Standards.

The Guidance for Suppliers

Making the Case

All business cases must become more sophisticated including a sound IT strategy to be aligned with an organisation' s clinical strategy as a future-proof investment. Detailed analysis must be provided that adheres to NHS contractual standards & obligations, clinical outcomes and service delivery and risk and information governance.

If the vendor' s business plan does not demonstrate an understanding of the clinical agenda in the procurement phase, not only is it less likely to be chosen to provide those services, but there is a risk of the technology becoming outdated, particularly if there are divergent developments in the clinical strategy e.g. a clinical shift towards increased integrated community care without appropriate infrastructure (i.e. remote access, network speed and suitable mobile devices) or understanding of clinical processes in the community, may result in technology which is not only out of date, but less suited to meet the demands of mobile working, and result in workarounds that compromise data security, as well as having limited returns on investment.

Realising Benefits at Scale

A business strategy involving baseline benchmarking not only provides valuable measurements to demonstrate the clinical and operational returns on investment to NHS trusts, but also helps identify any existing areas of concern regarding information governance and reduces associated risks.

Additionally, as the Review recommends that NHS Digital (formerly HSCIC) be central to standardising processes with data security, the importance of following the SCCI standards is paramount. Examination by a Clinical Safety Officer (CSO) of the IT solutions implemented, in terms of any associated risks, helps safeguard against any future repercussions in any data security incidents. The resources required to manage this can be substantial and require a dedicated team.

With disenfranchised frontline staff and human behaviour a key contributing variable to breaches, helping to bridge the gap between IT and clinical staff can improve this disconnect. IT suppliers that can engage clinical staff and demonstrate milestones which can illustrate these types of outcomes and not just technical achievements will stand out. Aligning supplier solutions with clinical staff through an engagement model will not only unlock necessary budgets and resources to support the successful procurement and adoption of solutions, but also enhance relationships with clinical stakeholders and decrease risks of human behaviour leading to governance breaches.

What does this all mean?

New standards with increased monitoring, responsibility and consequences may initially be of concern.

However, it is our prevailing view at AbedGraham that the findings of this Review consolidate the requirement for suppliers to engage clinicians and demonstrate a clinically led business strategy for clinical, financial, operational and governance benefits, and presents an opportunity for vendors who can adapt their commercial operations appropriately to be successful suppliers within the evolving health IT industry.

About AbedGraham

AbedGraham is Europe’ s leading, exclusively clinically based, healthcare IT strategy, operations and risk consultancy. The organisation’ s combination of clinical and strategic expertise is utilised by global IT infrastructure industry leaders to shape corporate strategies, clinical engagement and leadership initiatives, business case developments, major project bids and project management processes to maximise the positive impact of their solutions for healthcare providers. For more information, visit http://www.abedgraham.com or follow on Twitter at @AbedGraham.

Contact the Authors

Dr Saif F Abed BSc MBBS MPhil, Founding Partner, AbedGraham

E-mail: sabed@abedgraham.com

Dr Gabriel K Ma MBBS MRCPsych, Clinical Strategist, AbedGraham

E-mail: gma@abedgraham.com