CoreStream®

# In the Press

## Managing and protecting data in the NHS

*As featured in IT Pro Portal & Information Age*

**Expectations of the UK's National Health Service continue to rise, with mounting pressures from a government programme requiring billions of pounds in efficiency savings, and the strain placed on existing services by a rapidly increasing population.**

Smarter use of patient data has long offered the potential for more efficient and better-targeted services, but past projects have often ended as expensive failures. What's more, any technological improvement that allows us to better capture, record and analyse data, also increases the danger that it will be lost, stolen or misused – and patients are understandably concerned about the security of their personal details. As the world becomes ever more connected, and the value of this information to criminals becomes higher, their efforts to obtain it increase in number and sophistication.  How can health organisations obtain the information they need to improve services, while providing reassurance to consumers that their data won't fall into the wrong hands?

As it stands, healthcare is responsible for more data breaches than any other UK sector, and the number of cases is rising fast. There were 734 instances in 2014, and year-on-year numbers doubled from April-June 2013 to the same quarter the following year[1].  UK trends could be set to follow those of the United States, where 91% of healthcare organisations have suffered at least one data breach in the past 2 years, and 40% have suffered more than 5 incidents.  More importantly, mistakes and negligence are no longer the principle cause: criminal attacks on the healthcare sector have

[1] http://www.computerworlduk.com/news/security/data-breaches-in-uk-healthcare-sector-double-since-2013-ico-numbers-show-3589814/

# In the Press

increased by 125% since 2010[2]. Hackers can also steal far more information than is usually lost in error: the recent attack on Excellus is believed to have involved up to 10 million individual records[3].

In the UK, the Information Commissioner's Office (ICO) is responsible for upholding information rights and data privacy for individuals. The ICO investigated 517 data breaches in UK health organisations last year[4]. Most result in the organisation formally undertaking to comply with the ICO's rulings, but since 2010 serious breaches of the Data Protection Act have been punishable by fines of up to £500,000. Nearly £6.5 million in fines have been levied for losses of sensitive personal information, the majority coming from public sector organisations. The largest fine to date, £325,000, came against Brighton and Sussex University Hospitals NHS Trust in 2012[5].

The spotlight was placed firmly on the NHS in February 2015, when the ICO secured the right to subject public healthcare organisations to a compulsory audit. According to the Information Commissioner, "*The health service holds some of the most sensitive personal information available, but instead of leading the way in how it looks after that information, the NHS is one of the worst performers… this new power to force our way into the worst performing parts of the health sector gives us the chance to act before a breach occurs.*"[6] Meanwhile, fines could be set to increase dramatically once the EU's General Data Protection Regulation comes into force later this year. The new regulations set the limit for financial penalties at €100 million.

The Information Governance Toolkit is the Department of Health's response to the need for better control of sensitive information within the NHS and government authorities. All organisations with access to NHS patient data, whether part of the

[2] http://www.esecurityplanet.com/network-security/91-percent-of-healthcare-organizations-suffered-data-breaches-in-the-past-two-years.html

[3] http://www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html

[4] http://www.computerworlduk.com/security/nhs-tops-list-for-serious-data-breaches-last-year-3607138/

[5] https://ico.org.uk/action-weve-taken/enforcement/ and http://breachwatch.com/ico-fines/

[6] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/02/ico-given-new-powers-to-audit-nhs/

# In the Press

NHS or not, must provide assurances that they are practising good information governance and use the IG Toolkit to evidence this. Worryingly, surveys in February and March 2015[7] found that fewer than 40% of respondents felt the IGT met their needs. Many frustrations centred on the fact that the IGT is not kept up-to-date and that it isn't focused on the right things. Senior managers did not see the Toolkit as supporting good governance or as helping them to discharge their legal obligations. In fact, most organisations believe that they could devise a superior compliance regime themselves, although a surprising number felt that they shouldn't be assessed on the outcome.

Adopting a piecemeal approach would surely be a retrograde step. A better response is to accept that legal and regulatory bodies, and the public, are becoming much less tolerant of shortcomings in data security; and to use technology to maximise the value of the IG Toolkit content. NHS England has gone down this route by commissioning a new technology solution to manage its information assets. Live within three months, the Information Asset Manager (IAM) provides the management layer missing from the IG Toolkit, giving demonstrable control over information assets and data flows, and clearly identifying key risk areas. The result is a huge reduction in the administrative burden of Toolkit compliance; and minimisation of the risk of data losses – and costly fines – due to mismanagement and human error.

This proactive approach is perhaps an example where the public sector, and specifically healthcare, is leading the way. Following the successful introduction at NHS England, IAM is being rolled out to Northern Devon Healthcare Trust; and since 90-95% of IG Toolkit requirements are the same for most NHS organisations, it could be only a matter of time before others follow suit.

As always, the first step to solving a problem is knowing what the problem is.

"*Of course, no organisation should expect to purchase their information governance solution 'off the shelf.' After all, technology is only part of the equation; it allows the process and content elements to be monitored and managed in a more efficient and targeted manner, but those elements must also be right,*" says Richard Eddolls, Head of Platforms at CoreStream.

With that caveat, it's fair to say that tools like IAM provide a quick and cost-effective means of making significant improvements

[7] http://systems.hscic.gov.uk/infogov/iga/news/surveysexec.pdf

to information governance; and this should enable organisations to adopt an approach to data security and data utilisation that is fit for the 21st Century.

ENDS