Dear Dame Fiona,

As a global supplier of healthcare privacy auditing solutions for electronic health records, FairWarning® welcomes the opportunity to input into the Information Governance Review.

Electronic based healthcare is among the most important advances of our times. Its value is not in the treatment of a specific disease or condition, but as a powerful enabler, transforming how we plan and deliver care to individuals and populations. Electronic health records bring better, more sustainable healthcare and offer the NHS the opportunity to make large savings – allowing more public money to be invested in improving patient outcomes.

Current reforms to the NHS in England are giving local healthcare providers greater autonomy and responsibility for their own electronic healthcare systems – and for ensuring that they are fully secure.

Robust data protection is the bedrock of successful electronic healthcare. The free flow of information is essential for the sustainable delivery of better outcomes for patients – but this can only work if clinicians and patients have confidence that sensitive data is secure. The ability to protect patient privacy is therefore a vital component in building trust between patients and clinicians. Without it, public confidence will erode, and patients and NHS professionals may back away from electronic systems.

Studies suggest that improper access to patient records can do significant reputational harm to hospitals and damage the patient-clinician relationship. A recent survey of over 1,000 UK citizens revealed that 86.5% of respondents believe a serious breach of personal data would do considerable damage to a hospital's reputation. 87.2% believe the NHS should monitor who looks at their patient records.

Despite this, many NHS hospitals do not have systems in place to proactively detect privacy violation – and remain vulnerable to breaches, litigation and regulator fines.

Until it becomes mandatory for trusts to build patient privacy into NHS IT systems, the ever-present risk of major data breaches will remain – and the full patient benefits of electronic healthcare will not be realised.

It is against this background that FairWarning® would like to take the opportunity to offer its perspective on the critical issue of patient privacy, and to highlight what we believe should be the key considerations for the Information Governance Review.

Disclosure & notification

Recent data from the UK Information Commissioner's Office (ICO) reveals that data security breaches within the NHS have increased by 935% in the past five years. Yet there remains no legal requirement in the UK for providers to disclose to the patient when a privacy breach has taken place. This must be addressed. UK citizens have a basic right to know when their records have been inappropriately accessed and their privacy compromised.

The biggest driver for improvements in patient privacy will be tighter legislation around **disclosure and notification**. When a breach has occurred, **providers must be mandated to provide breach disclosure to**

patients, and breach notification to the ICO. This would bring a level of accountability to care providers that cannot be achieved by other measures such as random audits and fines.

Healthcare privacy laws in the rest of the world are being significantly strengthened – and the NHS cannot afford to be left behind. In the US, ARRA HITECH privacy legislation (2009) introduced – and enforced – strict guidelines around breach disclosure and notification. Similarly, in Europe, pending legislation in the General Data Protection Regulation will mandate the disclosure and notification of privacy breaches to individual patients and governmental organisations respectively. The NHS should rigorously enforce this legislation.

Mandatory audit trails

At present, there is no legal requirement for electronic health record vendors or applications used in healthcare to produce a robust audit trail. This means that when a privacy breach has occurred, neither the care provider, enforcement agencies or the patient has the ability to reconstruct who has been affected, to what extent damage has been done and how long it has been occurring.

Furthermore, the majority of providers are unable to identify proactively where privacy breaches have taken place – other than to wait until a patient reports concern. The current system provides no facility to audit, proactively discover or mitigate what has happened. In such an environment, it is impossible to determine the scope of the damages, or to proactively protect against them reoccurring in the future.

Mandating the use of audit trails across all electronic health records and applications used in healthcare would be the first and potentially most important step towards securing and protecting patient privacy.

Robust standards for audit trails

The implementation of robust standards for audit trails will be a key component in the delivery of an electronic healthcare model built on the principle of interoperable systems and widespread sharing of data. Interoperability increases the risk of security breaches and, as such, underlines the need for common and robust standards for audit trails to underpin all healthcare applications.

Based on its experiences of implementing breach monitoring and detection solutions all over the world, FairWarning® has developed an open copyright *Patient Privacy Data Definition Guide*. This has been widely adopted by major electronic healthcare vendors such as McKesson, Epic, MEDITECH, GE and Allscripts.

The culture of change

Effecting meaningful change is as much a cultural challenge as it is a technological one. FairWarning® agrees with the wider healthcare technology community that education, training and awareness of patient privacy within the NHS needs to be improved. The implications of security breaches must be fully understood across the health sector. Healthcare leaders must also become privacy leaders.

Clear guidelines are needed on information sharing and privacy in order to help healthcare providers put the right practical measures in place. Encouragement is also required to reinforce a culture of privacy. This can only be achieved if all organisations involved with NHS care implement three basic safeguards:

1. Secure electronic communications with patients and carers
2. Security of data in and across systems
3. Assurance of only appropriate access to data.

Our recommendations

In order to secure and protect the basic patient right of data confidentiality, FairWarning® recommends the Information Governance Review considers:

- Mandating trusts to build patient privacy into NHS IT systems
- Reinforcing a culture of privacy in the NHS through education and awareness
- Making healthcare providers fully accountable for breach disclosure to patients and breach notification to the ICO
- Enforcing the mandatory use of audit trails across all healthcare applications
- The introduction of robust standards for audit trails.

We believe that these simple steps will help to transform data security within the NHS, building levels of trust between patients and providers and significantly enhancing patient care through the secure use of electronic healthcare.

FairWarning® works closely with healthcare organisations all over the world, protecting patient privacy in over 900 hospitals across the UK, the United States, Canada and France. As a result of our experience in the provision of healthcare privacy auditing solutions, we would be happy to offer our expertise to the panel.

Sincerely,

Kurt J. Long
Founder
FairWarning®