Make or Break – Digital Healthcare and Privacy Reach the Tipping Point

A FairWarning® White Paper

Trust but Verify®

FAIRWARNING®

About FairWarning®

FairWarning® is the inventor of and global leader in Privacy Breach Detection and appliance-based software solutions which monitor and protect patient privacy in electronic health records enabling care providers and health information exchanges to confidently connect physicians, clinics, patients and affiliates. FairWarning®'s turn-key privacy auditing solutions are compatible with healthcare applications from every major vendor. FairWarning® customers represent nearly 900 leading hospitals and 2,600 clinics in seven countries and forty-three of the United States.

Notices

Copyright and Trademark Notices

The materials in this document and available on the FairWarning® web site are the property of FairWarning®, and are protected by copyright, trademark and other intellectual property laws.

TRADEMARKS

FairWarning®, the logo, Trust but Verify® and other trademarks of FairWarning® may not be used without permission.

MATERIAL FOR USE "AS-IS"

THIS FAIRWARNING® REPORT IS FURNISHED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND AND FAIRWARNING® HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES AS TO NON-INFRINGEMENT, AND IN NO EVENT SHALL FAIRWARNING® BE LIABLE FOR COSTS PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL FAIRWARNING® BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR DAMAGES WHETHER OR NOT FAIRWARNING® HAS BEEN ADVISED OF THE POSSIBLITY OF SUCH LOSS OR DAMAGE.

White Paper Executive Summary

Introduction

Attacks on patient privacy are of rapidly-growing concern in the UK. There are regular reports of serious data breaches by members of staff which can harm patients, damage the reputations of healthcare providers and erode confidence in electronic care.

Make or Break – Digital Healthcare and Privacy Reach the Tipping Point is a new white paper from FairWarning®, the inventor and global leader in privacy breach monitoring and detection for healthcare. It provides incisive analysis of the issues and how they affect key stakeholders, offering sustainable solutions which mean that healthcare providers can rest assured that the confidentiality of their patients is properly protected.

Executive Summary

Electronic healthcare is a liberating force for clinicians, healthcare providers and patients. It promises better care, delivered faster, with greater safety and improved outcomes. But there are dangers. Unless patient privacy is built into NHS IT systems at ground level there is the ever-present risk of major data breaches.

The greatest threat is not from lost or stolen laptops and mobile devices, but from staff abusing their legitimate access rights to read electronic records they have no right to see. This can lead to identity theft, fraud and many other forms of criminality. Details of celebrity patients can also be leaked to the media.

Improper accessing of patient records is widespread in the UK and worldwide. It can result in immense harm to the reputation of hospitals, their senior management and their clinicians and cause irreparable damage to patients and their families. Equally it can undermine the trust of patients, and the wider public, in the specific organisation and more generally in electronic health records.

This paper is the result of detailed research and global customer experience around privacy breach detection. It also includes extensive input from respected experts in UK healthcare and privacy regulation. Overall it provides an analysis of the problem and guidance on the way forward.

The privacy issue is considered from the perspective of key groups. These include **Chief Executive Officers (CEOs)**, for whom the reputation of their organisation is a precious asset. It is critical for them to protect against data breaches and maintain the faith of patients and commissioners. To achieve their goals, CEOs must guarantee that information can flow freely and securely, which demands sustainable and effective privacy protection.

Sustainable data protection is also essential to **Chief Information Officers** (**CIOs)** – it's the bedrock of successful electronic healthcare. Yet **IT**, **security** and **governance professionals** are aware that privacy breaches are common. Most UK hospitals do not have systems in place to prevent them. They are vulnerable to breaches, litigation and enforcement by regulators.

Automated record monitoring and privacy breach protection solutions are, however, readily available. They are already in use by NHS Scotland and by organisations overseas. This paper looks at the advantages they bring and also provides a wider privacy blueprint of value to IT professionals.

For **clinicians** it is essential that the information they gather about patients is secure. Data breaches threaten the trust between patient and clinician. Evidence shows that patients will delay seeking treatment, or fail to disclose important information to clinicians, if they are worried about lack of confidentiality. Many will also turn their backs on a particular provider and go elsewhere.

Patients expect the NHS to know who is looking at their records. They also fear that their families and jobs could be threatened by data breaches. They increasingly demand that those who are responsible for damaging breaches be held accountable.

Unless action is taken to ensure privacy then the future of electronic healthcare is at risk – so are the reputations of many providers, senior managers and clinicians. This needs to change so that patients, the public and healthcare professionals can feel confident and safe regarding their use.

Breaches and the Public Response

Recent media coverage has further highlighted the risks of patient privacy breaches by healthcare staff. This includes the Telegraph story of April 2012 which used Freedom of Information Act responses to show a doubling in the number of recorded security breaches involving patient data in the previous four years.

An independent public attitude survey of more than 1,000 UK citizens (conducted on behalf of FairWarning®) revealed widespread fears about privacy, plus a demand for firm action against senior management in hospitals where breaches took place.

The main findings of the survey included that:

- **86.5%** think that a serious breach of personal data would do severe or considerable damage to a hospital's reputation.
- Over **61%** were worried that a breach could allow their identity to be used to commit fraud or be used by criminals to target them, their family or home.
- **87.2%** agree that the NHS should monitor who looks at their files.
- **87.1%** agree that chief executives and senior management should be sacked or fined if they were aware of risks but failed to act and there is a serious breach.

Make or Break – Digital Healthcare and Privacy Reach the Tipping Point analyses the issues and shows how they can be tackled. Download it for free at www.FairWarning.com.

Overview

Contents

Introduction

Electronic healthcare is among the most important advances of our times. Unlike drug discoveries or new surgical techniques, its value is not in the treatment of a specific disease or condition. Its power is as an enabler, transforming how we plan and deliver care to individuals and populations.

Recent years have seen a tremendous expansion in the use of electronic health records (EHRs) in the UK. They bring better, more sustainable healthcare. They also offer the NHS the opportunity to make very large savings – allowing more taxpayers' money to be invested in improving patient outcomes.

However, EHRs are only as good as the information they hold. Clinicians must have access to all relevant data if they are to provide the best and safest care. In an era where specific consent is increasingly necessary for the collection and use of personal details, patients must have absolute faith that the doctors, nurses and institutions which treat them will protect their information. Reputation is a key factor in determining the success of EHRs. Those whose reputations have been tarnished by data breaches could find patients and commissioners less willing to use their services. Lack of trust can also lead to adverse outcomes as patients are less willing to seek timely treatment, or provide full details of certain conditions.

In a healthcare market increasingly predicated on patient and choice, and where clinical commissioning groups can make far-reaching decisions over providers, a good reputation is an asset of incomparable value. Unfortunately, the good reputations of most UK healthcare providers are at risk because their IT systems have an Achilles heel – they are highly vulnerable to data theft and fraud. At any moment they could find themselves confronted with a severe data breach.

Data security must be dealt with holistically as there are dangers from many sources. This demands that organisations train all their staff in privacy issues. They also need to have specifically named, trained and competent personnel who take direct responsibility for actively monitoring who is accessing electronic patient records. Another basic is the encryption of any data which might be placed on a portable device. It is also of the highest importance that organisations make sure that their applications comes with enabled and effective audit logs – and that these are switched on. Many healthcare providers are severely undermining their ability to safeguard patient confidentiality by leaving audit logs switched off.

The focus of this paper, however, is on the most significant data breach threat – which is also the least well known and most neglected. This comes from staff abusing their access privileges to search confidential patient records. It also explores how the problem can be mitigated effectively and sustainably by making a one-off investment in an appropriate privacy platform.

Patient data breaches by staff are dangerous on two levels. First, they directly harm patients, their families, and healthcare organisations. Second, they can lead to a damaging loss of patient, public, clinical, media and political confidence. At a time when there is a pressing need for more information to

be shared between ever-growing numbers and types of institution, the whole drive to make care more efficient and effective through advanced IT could be undermined. [1]

Loss of confidence in electronic healthcare could undermine progress towards many NHS objectives such as:

- The introduction of clinical portals and electronic records.
- The roll out of tele-health and tele-care technology to millions of patients, improving care and cutting costs for long-term chronically ill people, who consume a disproportionate amount of the health budget. [2]
- The target for all patients in England to be able to access their GP records electronically by 2015.

The UK health service is at a tipping point. Enormous and beneficial changes are possible. But their success is threatened because vast quantities of sensitive personal information are being exchanged among large numbers of clinicians and healthcare providers through IT systems which are fundamentally insecure.

Legislators and regulatory bodies are increasingly aware of privacy issues. At national and European levels we are seeing a tightening of laws, with more emphasis on the rights of citizens to have their information protected. [3] Regulators are also becoming more willing to impose sanctions for breaches. [4]

Given the rapid and dramatic changes, it is vital for healthcare leaders to make sure they also become leaders in privacy. More broadly, privacy protection is an issue for everyone – especially for board members, IT specialists, clinicians and patients.

[1] The impact of security worries can be seen in both Germany's 2010 suspension of the proposed national e-health smartcard (EHI, 10 January, 2010 www.ehi.co.uk/news/primary-care/5551) and in the UK with the plans for a national identity card (BBC, 8 June, 2010 news.bbc.co.uk/1/hi/uk_politics/7441693.stm) which were abandoned in 2011 (Computing.co.uk, 24 Jan, 2011, www.computing.co.uk/ctg/news/1938962/road-id-cards).

[2] In England this is exemplified by the recent launch of the 3million Lives project (See www.publicservice.co.uk/news_story.asp?id=18224).

[3] See ec.europa.eu/justice/policies/privacy/review/index_en.htm.

[4] *Promoting openness by public bodies and data privacy for individuals* can be accessed at www.ico.gov.uk/about_us/plans_and_priorities/information_rights_strategy.aspx.

Privacy and the Chief Executive

Key Points

- Reputation is a precious asset – protecting against data breaches is essential to maintain the trust of patients and the confidence of commissioners.
- The free flow of secure electronic information is essential for better, safer care – this demands sustainable and effective privacy protection.
- The CEO and senior management team are the public face of a healthcare organisation – a privacy breach puts their credibility on the line

Better Care Means an Electronic Future

Every NHS chief executive and board member faces huge challenges, with an urgent need to do more with less. Electronic healthcare systems offer a chance to do this. They are especially valuable in an environment where providers have to cater for a burgeoning older population and a rapid increase in long-term and chronic conditions.

EHRs, and multi-organisational health information exchanges (HIEs), will be fundamental to every healthcare provider's work to offer safe and sustainable care. Increasing convergence and collaboration between organisations (and in some cases mergers), mean that the greater electronic sharing of patient information offers a route to cutting costs and improving performance.

Equally, in an ever-more competitive environment, EHRs are essential to running a successful business. As patients and commissioners look at which providers to choose, their decisions will be powerfully influenced by whether they trust the staff and the institution to protect their personal information. The protection of data is becoming essential to the delivery of world-class care.

Building a Culture of Respect and Trust

EHRs provide the capacity to do enormous good. The power to collaborate on patient care across extended teams, based at different sites, working a variety of shifts, and often employed by different organisations, is an immense plus for patients and providers. With this collaborative power comes a matching responsibility to ensure that patient privacy is respected and protected.

Healthcare providers also have to ensure that they comply with laws and regulations. Evidence gathered in the UK and overseas by FairWarning® (and by other organisations [5]) shows this is not happening. On any given day a typical large hospital can expect inappropriate accessing of patient records by staff three to five times. This is because too few have a sustainable and effective automated monitoring system to detect breaches. The problem was highlighted by a BBC investigation which led to the statement that 'Patients' confidential medical records are regularly being accessed by people who have no right to them.' [6]

Levels of inappropriate accessing rise dramatically in certain situations – the arrival of famous or infamous patients, or a substantial intake of new staff. Any breach is dangerous and can lead to:

[5] See 2011 Gaurdian interview with Information Commissioner Christopher Graham who says privacy procedures are not being followed by NHS staff (www.guardian.co.uk/government-computing-network/2011/jul/01/information-commissioner-christopher-graham-warning-data-loss-nhs).
[6] See news.bbc.co.uk/1/hi/England/Bristol/7119075.stm.

- Reputational damage – with management seen as incapable of protecting privacy
- Direct harm to patient outcomes
- Loss of trust by clinicians and patients
- Sanctions by regulators or legal action
- Fraud and other criminality
- Damage to patients' private and professional lives
- Negative headlines and media stories
- Increased costs for readmission / improper treatment

Serious breaches can raise questions about senior management. A UK survey showed that 87% of respondents believe that chief executives and senior management should be sacked, or fined, if a serious breach takes place when they were aware of the risks and failed to act. It also revealed an overwhelming view (86.5%) that a serious breach of personal data would damage a hospital's reputation. [7]

Effective counter-measures must be in place, both to deal with immediate problems and (more important in the medium to long term) to build a culture of respect and trust. This is the most effective tool which CEOs have in overturning a culture where certain staff think that casual intrusion into confidential details is undetectable. NHS Scotland, which leads the UK with its ongoing rollout of breach monitoring and detection measures, is successfully strengthening the culture of respect. [8]

Worldwide experience shows that it is preferable for organisations to introduce monitoring at their own pace, which keeps them in control of events. NHS Scotland has employed a well-planned strategy which combines the use of technology, internal communications and HR management to show staff that breaches can be detected and will not be permitted. Most abuse stops straight away, making way for a stronger culture of respect for privacy. Incidents do continue, but organisations are well equipped to identify and deal with them. English hospitals can also look to the successful piloting of privacy software in Wales to see what can be achieved, as well as the examples being set in Canada, France and the USA.

The uncomfortable alternative, as growing numbers of NHS CEOs and their boards are finding out, is to be forced to act after experiencing the damaging and difficult process of cleaning up after a severe breach. [9] A breach of the Data Protection Act (DPA), for example, led to the CEO of NHS Birmingham North East signing a public undertaking to ensure that adequate technical security measures were put in place to prevent unauthorised access to personal data. [10]

Privacy Protects the Patient and Provider

CEOs and senior management teams can protect their patients and staff, and the reputations of their organisations, with automated and sustainable data monitoring. The UK survey cited above showed widespread public acceptance of monitoring with 87.2% of respondents agreeing that the NHS should know who looks at their files.

---

[7] The survey had more than 1,000 respondents and was carried out by New London Consulting. It was commissioned by FairWarning in 2011. For the full results see *How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* at www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

[8] For detailed information see www.fairwarning.com/documents/2011-WHITEPAPER-HIE-NHS-SCOTLAND.pdf and the video case study of NHS Scotland www.fairwarning.com/videos/2011-VIDEO-NHS-LOTHIAN.html.

[9] In January 2012 Praxis Care Ltd made a commitment to the ICO to encrypt all data after breaching the DPA when a memory stick was lost (see www.ico.gov.uk/news/latest_news/2012/action-taken-after-care-provider-lost-unencrypted-memory-stick-18012012.aspx).

[10] See ICO website www.ico.gov.uk/news/latest_news/2011.aspx.

EHRs, and the associated supporting technologies, are the bedrock on which the future of the NHS is being built. [11] At the moment they promise financial affordability, but they must be bullet proof in privacy terms, otherwise the reputational costs could be unaffordable. When boards have so many other responsibilities they do not need the distraction of failed security audits, patient law suits and negative headlines.

The manual monitoring systems on which many hospitals rely (and which IT departments know are largely ineffective despite being resource intensive) must be replaced with automated ones that are effective and sustainable. CEOs can then ensure the secure and private collaboration of doctors, nurses, therapists and every other member of the care team. This in turn protects and enhances their reputations for caring for, and protecting patients.

Unfortunately the Information Commissioner's Office (ICO) fears there is a danger that healthcare organisations could back away from security measures because finances are tight. [12] This is a false economy at a time when patient and commissioner choice is growing and providers must defend their reputations. Those who do not trust an organisation with their data may simply go elsewhere. [13] Similarly, there is an increasing chance that patients could refuse to let organisations hold data about them. The success of electronic healthcare also depends heavily on its acceptance by clinicians. There is a real risk that they will block, or back away from, systems they do not trust. This cannot and need not happen, so long as prompt action is taken.

To ensure the free flow of electronic patient information (as the means to deliver better, safer care), CEOs and senior managers must act fast to introduce proper privacy breach detection. This is vital if they are to protect the reputations of their organisations and staff, as well as to protect patients and to avoid the damage which can be caused by negative headlines following a severe data breach.

In their own words – the NHS IG Lead

"NHS healthcare is changing rapidly, with a huge increase in the amount of patient information being shared by integrated care teams across different organisations. This brings enormous benefits to the delivery of quality healthcare, but patient confidentiality must be protected. Our concern at NIGB is to make sure that everyone involved in delivering care understands their duty to protect the confidentiality of personal information and that every organisation has the right procedures and systems in place to ensure that sensitive data is secure.

"It is essential to maintain public trust in the NHS. If people fear that their personal details are not secure there is a risk that they will withhold information from clinicians that may be vital to their treatment. At present people have faith in the NHS to deliver a confidential service and we want this to continue. But there are many potential challenges with new organisations being commissioned to provide healthcare services and the major developments that will flow from new strategies set out in the Information Revolution where the Government makes it clear that patients will have control of their own health records starting with access to their GP record by 2015.

---

[11] The Joint Working Group (JWG) established by the DH Informatics Directorate recently declared that the patient record 'is likely to become the single most important unit of information in the NHS'. See www.rcplondon.ac.uk/sites/default/files/devoloping-standards-for-social-care-records-report-of-joint-working-group.pdf.

[12] See ICO Commissioner Christopher Graham's blog at www.ico.gov.uk/news/blog/2011/information-rights-in-a-cold-climate.aspx.

[13] The FairWarning public attitudes survey showed that data breaches would make 61.5% of respondents want to seek treatment at another hospital. Of these 37% would travel 30 miles or more, including 12.4% who would travel 50 miles or more. See www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

"Standards must be upheld, best practice shared, and improvements made wherever healthcare providers are falling short of these expectations. Providers need to be sure that they can meet their obligations for good data governance, and for patients' rights. This is set out in the Care Record Guarantee which says: "You have the right to privacy and confidentiality and to expect the NHS to keep confidential information safe and secure (NHS Constitution for England 2010)" and the NHS uses a combination of working practices and technology to keep this guarantee.

"In order to be fully transparent and trusted, providers must make sure that staff are properly trained in privacy policies and practice. Providers also need to make sure their patient record systems are fully secure. In this way they can protect trust and work in partnership with patients to deliver the best possible care."

Debbie Terry,
NHS Information Governance Lead,
National Information Governance Board for Health and Adult Social Care (NIGB)

CIOs: Better Care by Delivering on Privacy

Key Points

- Sustainable, effective data protection is the bedrock of successful electronic healthcare.
- Privacy breach detection and deterrence protects the reputation of healthcare providers and their senior management.
- Immediate action is needed to meet obligations on patient privacy.
- Effective privacy protection software can also detect fraud.
- Senior managers are the public face of a healthcare organisation – a privacy breach puts their credibility on the line

Privacy as a Priority

Chief executives and their boards rightly want healthcare delivery that is based on affordable and patient-centred EHR platforms which feed into specialist technologies, and which allow borderless collaboration for care teams. This is challenging to achieve as these advances must be delivered within a context of growing concern about the protection of patient information. The reality is that healthcare IT systems tend to be fundamentally insecure as there is no built-in software to detect privacy breaches by authorised staff using access privileges to obtain information they have no right to see. This can lead to patient data privacy breaches which can do massive reputational damage to healthcare providers.

In addition to their electronic patient record systems, modern healthcare providers are likely to be using dozens of other applications (often specialist systems), which can be accessed by hundreds, or thousands, of users. These will generate millions of transactions. In such circumstances effective manual monitoring is impossible. This means that an effective, automated system is fundamental to safe working practices, effective data governance and to meet regulatory and legal requirements.

Without effective breach detection systems CIOs cannot simultaneously ensure:

- Clinical access to all relevant patient data *and*
- The detection of abuse by staff.

Public concern has been fuelled by a succession of media stories which have revealed the absence of effective measures to prevent the theft and loss of data. This was demonstrated in 2011 when a Freedom of Information request by *The Guardian* revealed 899 breaches at 30 London trusts. [14]

Legislators and regulators are increasingly focused on enforcing confidentiality. The European Commission is currently tightening the law to make information holders more accountable and to toughen the penalties they face for failing to protect personal information. [15] The ICO has also stated that it will 'actively seek out situations where organisations significantly fail to live up to their information rights responsibilities and use the full range of our powers to address these'. [16]

With privacy becoming a central issue at the very time when the widest possible sharing of information is being recognised as a central tenet of healthcare, CIOs must be confident that IT systems combine flexibility with security. Unless they invest in software to monitor who is accessing electronic files then it

[14] The breaches took place from 2008-11. The numbers were highest at NHS Barnet and Chelsea and Westminster Hospital Foundation Trust. The article concluded that most breaches were avoidable (see www.guardian.co.uk/healthcare-network/2011/may/04/nhs-barnet-187-data-breaches-staff).

[15] See ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf.

[16] See Promoting openness by public bodies and data privacy for individuals at www.ico.gov.uk/.

is impossible to deliver the best care for patients, while protecting the reputation and integrity of their own organisation.

Growing Reputations

CIOs are on the front line when it comes to protecting and enhancing a healthcare provider's reputation. Perhaps more than any other individual the onus is on them to be the guarantors of data security, while simultaneously delivering a more sustainable future through the greater use of electronic care. If their IT systems are secure then patients will continue to provide sensitive information to clinicians, who can then give the best care. If patients are worried about breaches then they are less likely to be open, and may even go elsewhere for treatment.

At present a majority of the public (63.2%) still believe the NHS is committed to protecting their personal data. Yet substantial numbers have concerns, with 29.4% believing their hospital does not have proper privacy safeguards. [17] These perceptions are not helped by a steady stream of cases, some ending up in court, which revolve round repeated inappropriate accessing of patient records by staff. Examples include: [18]

- NHS Bury warned that details of 189 walk-in centre patients may have been leaked to personal injury lawyers.
- At Sheffield Teaching Hospitals a member of staff was caught looking at records of an ex-partner's new partner.

The dangers of failing to ensure that systems are secure, and the potential for reputational damage, were highlighted in January 2012 when Brighton and Sussex University Hospitals NHS Trust faced the possibility of becoming the first NHS trust to be fined (a projected £375,000) by the ICO for breaching the Data Protection Act. [19] Such actions by the ICO have strong public backing, with 73.3% thinking that better enforcement of regulations would cut security breaches and 55.8% feeling that existing laws are not adequately enforced. [20]

Clinicians, boards, regulators and the public rely on CIOs to make sure that these kinds of problems do not occur and that their systems comply with national and international requirements. Modern monitoring software can address the problem very effectively. It requires a single and straightforward implementation which then provides a good return on investment (ROI). This replaces slow, ineffective and resource-intensive manual monitoring processes with one that is fast, effective, resource-light and automated. It works by identifying patterns of access by individual staff which are legitimate and others which may be suspicious. Such software not only identifies potential snooping, but is also an excellent way to uncover another substantial problem – fraud.

It has often been thought that because the NHS is free at the point of delivery that it is less prone to fraud than other healthcare organisations. [21] Yet a recent report, supported by 2020 health, estimated

---

[17] For the full results see *How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* at www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

[18] For further details see www.phiprivacy.net/?p=6757, www.ehi.co.uk/news/acute-care/6549/nhs_trusts_report_unlawful_record_views. The walk-in centre case was linked to the death of former nurse Dawn Makin and the murder of her four-year-old daughter menmedia.co.uk/manchestereveningnews/news/s/1422178_probe-into-patients-names-leaked-to-personal-injury-lawyers-linked-to-mum-of-murdered-four-year-old-chloe-makin.

[19] See EHI, 24 January, 2012 www.ehi.co.uk/news/acute-care/7447/brighton-faces-fine-for-drives-on-ebay). Weeks before the ICO had revealed it planned to toughen its stance on breaches (ICO, 28 December, 2011 www.ico.gov.uk/news/blog/2011/information-rights-in-a-cold-climate.aspx.

[20] For the full results see *How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* at www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

[21] One case involved a UK nursing manager who defrauded the NHS of £125,000 by adding several members of her family to the payroll, see www.ehfcn.org/fraud-corruption/examples/healthcare-providers/hospitals/.

that the annual cost of NHS fraud could be £3 billion (the official estimate is £165 million). [22] While some forms of fraud are hard to identify, others can be readily picked up because they will involve readily detectable patterns of access to patient data.

As the NHS changes, with many new providers being brought in, and information of all kinds being exchanged through longer and wider networks, the potential for fraud and inappropriate accessing of patient records is rising. [23] Under these circumstances it is essential to ensure that every organisation is properly protected as soon as possible. For CIOs this is a readily achievable objective. It demands a single investment in breach monitoring software, which will immediately satisfy the demands for effective security to provide the bedrock for the safe expansion of electronic healthcare demanded by CEOs and governing boards.

Privacy breach detection software will allow CIOs to be sure that care teams can share information across many IT systems and organisational boundaries, and provides essential protection against fraud. In an environment of growing concern about privacy, it also allows them to be sure that their organisation is compliant with the growing demands of legislators and regulators.

In their own words – the Information Professional

'With the end of the national programme and the restructuring of the NHS, trusts are being pushed to gather and crunch massive amounts of sensitive personal data. It is anticipated that sharing and exploiting patient data will deliver greater efficiency and significant savings.

'This must not be achieved by compromising the moral and ethical responsibility to ensure patients do not have their rights thoughtlessly abused. However, the rapid adoption of new technologies has not been matched by equally powerful organisational controls.

'I know all too well that trusts struggle to honestly deliver confidentiality audits (IGT requirement 206) of complex systems which handle tens of thousands of transactions processed by thousands of staff daily. Nevertheless, the first NHS body has been fined by the ICO and more are likely to follow.

'Organisations need to accept the great responsibility that comes with their great power. I recommend any organisation implementing a new system to incorporate compensating controls into projects from the beginning. Organisations have already done this in Scotland using the FairWarning® privacy auditing solutions for Electronic Health Records. I know of no other product that can do this.'

David Stone
Principal Consultant
Kaleidoscope Consultants Limited

In their own words – the NHS CIO

'As an NHS CIO, from a clinical background and with extensive experience in the USA, I see the importance of patient privacy from several perspectives. Everything now suggests that the kind of stringent regulatory demands (and risk of sanctions) that has developed in America will soon exist over here. With this is mind I am convinced that early action to introduce effective electronic monitoring of patient records and breach detection is essential. It's far better to get ahead of the game and be

[22] See 2020health.wordpress.com/2011/11/14/1668/. In Scotland, around £43 million in net savings have been generated by NHSScotland Counter Fraud Services between July 2000 and 2011 www.scotland.gov.uk/News/Releases/2011/11/18162921.

[23] The Medical Protection Society has expressed concern about this issue saying: 'We believe effective communication between healthcare professionals could become more difficult as more providers enter the market.' (see www.medicalprotection.org/uk/check-up-october-2011/access-all-areas).

compliant now than to wait for a serious data breach and risk censure by the CIO or fines under the DPA.

'There is a rapid movement towards more patient information being exchanged, shared and updated by expanding groups of people. Soon there will be a free flow of data between primary, secondary and social care – and beyond to patients and careers themselves. In this situation I have to be absolutely certain about who is looking at what and whether they are doing so for legitimate reasons.

'Employers, clinicians and the public fully expect that the NHS will do its utmost to keep patient information confidential. In an electronic era much of the responsibility for this rests with the CIO. The challenge, however, is to create monitoring systems that are both effective and sustainable. My experience shows that this is possible, and that by using the appropriate technology the NHS can not only detect and deter data breaches but can actively strengthen the culture of confidentiality.'

Dr. Zafar Chaudry, CIO,
Liverpool Women's NHS Foundation Trust and
Alder Hey Children's NHS Foundation Trust

IT, Security and Governance Professionals: A Blueprint for Privacy

Key points

- Privacy breaches are common, but the systems are not in place to prevent them.
- All healthcare providers need to implement a privacy blueprint.

Effective Data Breach Monitoring

Healthcare IT, security and governance professionals are well aware that staff regularly access patient records they have no right to look at. This is a clear threat to privacy and can result in severe consequences for patients, staff, the departments involved, and for the organisation as a whole.

Most breaches are to find information about family and others the staff member knows personally, rather than about celebrities. It is not always clinicians who are responsible, but sometimes other trusted individuals. ***IT manager Dale Trever, 22, admitted accessing the records of 413 women a total of 597 times including family, friends and colleagues, while at Hull Primary Care Trust.*** [24] Each case emphasises the need for effective software to deter and detect privacy breaches.

Most existing IT monitoring barely scratches the surface. It shows that a problem exists, but is too slow and resource-intensive to resolve the issue. This leaves the organisation highly exposed to a known risk, and open to the accusation that it failed to take adequate preventative measures if, and when, something goes severely wrong.

A better approach is needed to comply with expected standards of confidentiality. These include the requirements outlined in the Information Governance Toolkit, which allows NHS organisations and partners to assess themselves against Department of Health policies and standards. The IG Toolkit makes it clear that organisations must have robust and effective measures in place. It demands: [25]

- Appropriate confidentiality audit procedures to monitor access to confidential personal information.
- An information governance agenda supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs.
- A formal information security risk assessment and management programme for key information assets to be documented, implemented and reviewed.

Meeting these standards is not possible without a sustainable system to identify the inappropriate accessing of patient records by those who have legitimate access to IT systems.

The ICO has published an information rights strategy which takes a firm approach to privacy breaches. While emphasising that prevention is better than cure, it states that they intend to make effective use of enforcement. [26] This follows repeated reports which have highlighted the number and severity of reported data breaches within the NHS. [27]

---

[24] See www.thisishullandeastriding.co.uk/NHS-manager-Dale-Trever-snooped-patients-medical-records/story-11953190-detail/story.html.

[25] See www.igt.connectingforhealth.nhs.uk/RequirementsList.aspx?tk=64&lnv=4&cb=17%3A55%3A44&sViewOrgType=15

[26] *Promoting openness by public bodies and data privacy for individuals* can be accessed at www.ico.gov.uk/about_us/plans_and_priorities/information_rights_strategy.aspx.

[27] The ICO warned the NHS it must do better at protecting patient information after revealing that four trusts had breached the DPA while a fifth had broken privacy laws (ZD Net, 1 July, 2011). The ICO announced that 14 trusts had breached the DPA in the previous six months (Computer Weekly, 30 April, 2009).

A Blueprint for Privacy

Privacy issues are best dealt with on a strategic/holistic and planned basis, rather than piecemeal or in response to crises. By working to a blueprint (like the one suggested below) it is possible to stay ahead of the curve – compliant with present and forthcoming regulations and providing security standards which give confidence to patients, clinicians and the board.

It is essential to meet the requirements of the DPA [28] and reflect (and extend), the principles set out by NHS Connecting for Health. [29] Information must be:

- Secured against unauthorised access.
- Monitored for inappropriate accessing by authorised staff.
- Safeguarded against unauthorised modification.
- Accessible to authorised users as required.

This demands that:

- Systems are designed and organised with security to fit the nature of the personal data held and the harm that may result from a security breach.
- There is clear responsibility for ensuring information security.
- The right physical and technical security exists, backed up by robust policies and procedures and reliable, well-trained staff.
- Organisations can respond to security breaches swiftly and effectively.

Privacy Blueprint: Strategy

A clear strategy, with specific budget and resource allocation, needs to be established. Six elements are essential for this to be effective:

1) Responsibility for data protection needs to be given to specific named staff
2) All staff have to be trained and competent in privacy issues
3) Information which could be transferred to portable devices must be encrypted
4) Organisations must insist that vendors supply fully enabled audit logs with their software
5) Healthcare providers have to make sure the audit logs are switched on
6) Automated privacy monitoring has to be introduced – and needs to be run by trained and competent staff.

If any of these elements is missing the organisation will be dangerously exposed. For example, many organisations currently have IT with audit logs, but choose not to switch them on. This severely limits their ability to understand who uses information in the custodianship of the organisation or how. And without activated audit logs they cannot make use of the privacy breach monitoring software which is fundamental to their ability to prevent staff from abusing their access rights to sensitive patient information.

Smooth privacy monitoring implementation is best achieved through a staged approach which involves:

- Running a gap analysis to identify security weaknesses.
- Ensuring that senior management are kept fully and regularly aware of gaps in security, the risks these bring and how they can be dealt with.
- Creating and implementing a written privacy and security plan.
- Targeting the largest areas of vulnerability first.
- Beginning a remediation process – the unannounced introduction of privacy breach detection software to identify the extent and nature of the problem.
- A communications drive to inform staff that monitoring is now taking place, backed with evidence to demonstrate its effectiveness.
- A clear restatement by HR of policies and responsibilities for confidentiality.

[28] ICO website www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx.
[29] See www.connectingforhealth.nhs.uk/systemsandservices/infogov/security.

- Ongoing staff education and training in privacy issues and compliance.
- Regular internal audits on regulatory compliance.
- HR meetings to advise staff who are continuing to breach patient privacy.
- Regular restatement of policies and reminders that monitoring is in place.
- Taking swift action over remaining breaches.
- Conducting an organisational IT security risk assessment at least once a year.

This positive strategy keeps the organisation in charge of events and eliminates most problems without formal disciplinary action. Breach monitoring and detection empowers the organisation to decide how to deal with each breach.

Privacy Blueprint: Technologies

Data security requires specific technologies. Every IT system should already be protected against unauthorised access. Encryption should also be standard to prevent data being accessed if portable devices fall into the wrong hands.

This leaves one main area of vulnerability to be tackled – the detection and deterrence of inappropriate accessing of records by staff. Breach monitoring and detection software deals with this. In fact, it addresses a whole series of incident categories – in some cases no other technology is effective. These include:

- Co-worker/patient snooping.
- VIP medical record access.
- Financial identity theft.
- Medical identity theft.
- Inappropriate physician access.
- Neighbour snooping.
- Compromised application user IDs.

Choosing which privacy breach detection software to use is of vital importance. The key features which must be present include:

- The capacity to handle very large numbers of transactions in real time.
- Scalability, so it can adapt to growing regulatory demands.
- The ability to audit new applications.
- The ability to incorporate additional patient data for reporting and analytics.

Breach monitoring brings cost-effective and immediate gains, allowing the identification of breaches which previously went undetected (FairWarning®'s evidence suggests a ratio of 4:1). Once the fundamentals are in place then other approaches and technologies can bring additional benefits – all are valuable, but none deal with authorised staff using legitimate access.

Identity management and provisioning assists with credentials management and fills a gap related to denying access to former employees. Security information management (SIM or SIEM) technology collects information security events from infrastructure systems such as firewalls, routers, IPS, IDS, servers and VPNs.

Privacy Blueprint: Outcomes

In most cases no healthcare provider needs to be caught out by a security breach, or to fail privacy protection audits. By replacing manual checking processes with automated ones, they can achieve compliance with legal and other obligations. This allows resources to be reallocated. Indeed privacy breach detection is quick and straightforward to introduce.

Experience shows that a positive engagement with staff on privacy issues reinforces a culture of respect for confidentiality and builds confidence in IT systems. The knowledge that records are being monitored produces a large drop in misuse, leaving the organisation to focus on the hard core.

Among the potential gains is the capacity for the rapid resolution of complaints and queries - which may well increase in coming years. The EU wants data holders to report breaches with the minimum delay, while giving patients quicker access to information about themselves and how it is being used, or misused. In the case of a media enquiry about a breach it is also essential for organisations to assemble an informed response within hours if they are going to meet journalists' deadlines and give their side of a story.

Automated monitoring allows hospitals to identify whether a breach occurred in their organisation, or elsewhere. It also lets them provide firm evidence of what has happened. Most important of all, effective breach monitoring and detection drives problems down to a minimum, protecting the organisation and patients from harm.

IT, security and governance professionals operate under an increasing weight of expectation and legislation. Only by using effective privacy breach detection software they can comply with regulations and public expectations, while enhancing healthcare:

- *ICO: 'We will promote the need for effective records management as a foundation for good information rights practice.'*
- *Information Revolution summary of consultation responses: 'Clear governance and consent models [are needed] to ensure the balance between accessibility and data security for this very personal information.'*

In their own words – the NHS IT, Security and Systems Professional

"2012 has seen an increase in the number of NHS Trusts procuring and implementing EHRs and portals. Many of these procurements are joint undertakings with neighbouring health organisations to facilitate the treatment of patients across traditional health boundaries, with patient information increasingly being shared between health, education, housing and social services through clinical and other portals. The requirement for EHRs to be available 24/7 wherever the patient may present, either within a Trust or requiring services from non NHS partners, adds complexity to the NHS' task of providing privacy and confidentiality.

"Currently patients believe in the NHS to maintain the confidentiality of their records. This perception is unlikely to continue if the NHS has further breaches of confidentiality. To achieve this it is necessary to monitor all access to the patient's data whether that is occurring within or outside the traditional boundary and that all such access is appropriate. Whilst role based access controls can assist in achieving this, many breaches have occurred where those controls were correctly applied, but then abused by individuals. It is therefore necessary to check each and every encounter for appropriateness. The need to check multiple data sources, to cross check applications and staff access becomes increasingly time and resource intensive.

"It is therefore essential that some form of automation linking the EHR, Portals and other clinical applications is implemented, providing monitoring between these systems and the interaction of staff measured against the organisations rules for appropriate access. Linking this monitoring to staff records can guard against snooping into colleagues or neighbours records. It can provide information on who may have been trawling multiple records, provide the patient a composite list of who was accessing their record, thus meeting the Care Record Guarantee needs in seconds and reducing the time IG teams spend at present on investigations and reporting.

Ted Boyle
Specialist healthcare IT consultant and former Systems Administration and Security Manager at NHS Lothian; Thorndene Consultancy

Clinicians: Confidence and Care

Key Points

- Patients must be confident that their personal information is safe with clinicians if they are to seek timely treatment and talk openly.
- As guardians of patients' interests, clinicians must be certain that IT is secure.
- Data breaches can seriously threaten the relationship of trust between patient and clinician.
- The reputation and credibility of clinicians can suffer if confidential information is insecure and falls into the wrong hands.

Privacy and Outcomes

Patients trust clinicians – for the sake of their health they need to. Almost every contact with a doctor, nurse, therapist or other member of a care team involves an act of faith – sharing the most sensitive details about themselves and their lives with someone else. There are times when the clinician is the only person in whom a patient feels able to fully confide. The trust they are shown is equal to, or even greater than, that which a patients shows to their dearest family and friends. And ultimately the trust they show is not just in the individuals they meet but in the entire care providing organisation.

The credibility and reputation of any clinician depends heavily on patient trust. If this is lacking their ability to provide the best patient care can be compromised. Patients may also choose to seek help elsewhere if they feel the confidentiality of their relationship is uncertain or think it has been compromised.

In an age of electronic data storage and exchange, where large numbers of people have access to immense quantities of sensitive information, patient trust must be protected from abuse. Leaks of information can be highly damaging to a patient's family or professional life, as well as exposing them to crime.

Clinicians are already aware of the challenges involved in encouraging people to come forward who might have conditions which attract stigma. A UK survey shows that 53.6% of respondents have, or would, withhold information about a sensitive personal medical matter from a healthcare provider with a poor record of protecting patient privacy. Some 38.3% have, or would, put off seeking care for a sensitive medical condition due to privacy concerns. In addition 72.9% said that serious or repeated privacy breaches would reduce their confidence in the quality of care provided by a hospital. [30]

Healthcare professionals can only order the right tests and determine the most appropriate course of action if patients have the confidence to tell them everything they need to know. Where a healthcare professional is seen as responsible for abusing personal information their reputation can be destroyed.

- In 2012 Cancer nurse Jennifer Ramsay (37), based at Dundee's Royal Victoria Hospital, admitted she was no longer fit to practice and was struck off after inappropriately accessing, and discussing, patient records at least 10 times. [31]
- In 2011 a staff member from Northampton General Hospital was sacked after accessing the health records of an acquaintance, a second person was severely reprimanded. [32]

---

[30] See *How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* at www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

[31] See news.stv.tv/scotland/tayside/297671-nurse-struck-off-for-snooping-on-files-of-patients-and-friends/.

[32] See www.phiprivacy.net/?p=9021.

Reputational damage may well go beyond the individual, affecting the entire institution for its failure to have effective detection measures in place. The impact is not just on the sense of trust, but on perceptions about quality of treatment. Nearly 73% of British people say that serious or repeated privacy breaches would reduce their confidence in the quality of care offered by a hospital. [33] This emphasises how anything which harms the patient's relationship with the healthcare organisation can potentially damage the relationship with the clinician.

The growing recognition of the need to protect information was made clear in the responses to the Westminster government's consultation on the Information Revolution white paper: [34]

- Cambridge University Hospitals: 'Recording information – whether clinical or administrative should be seen as an integral part of patient care …'
- Royal College of Nursing: 'there must be safe and secure ways to integrate clinical information from different electronic records across all providers and pathways so that a patient's healthcare is managed safely and effectively …'

By installing software to monitor who is accessing patient files and when, the patient and clinician are protected. It gives a full audit trail, proving the integrity of any individual clinician.

This kind of software helps maintain the vital relationship of confidence that must exist between care provider and patient if they are to deliver the best outcomes. Once the accessing of patient records is properly monitored, clinicians can have confidence in the free flow of patient information because they know that every member of any care team is aware that privacy is taken seriously. This in turn allows the safe expansion of electronic care into new areas.

Making Privacy Work

Clinicians must be able to access information fast. Multiple logins and complex security procedures are not compatible with a health service where clinicians have to work fast, and it is imperative that technology is an enabler rather than an obstacle to care. At the same time they have to be sure the systems they are working with are secure. Indeed, there are circumstances where clinicians could face severe ethical and practical dilemmas about making use of an IT system which has, or could be, compromised.

With respect to doctors, the Medical Protection Society states that the duty of confidentiality goes beyond not divulging confidential information themselves. They are also expected to be sure that such information is held and shared securely. The society points out that while confidentiality is often seen as an ethical issue, it is also a legal principle. It points out that: [35]

- NHS employees will find a confidentiality clause in their contract.
- There is a common-law duty to preserve professional confidence.
- It is a condition of doctors' registration to abide by GMC guidance, which includes a requirement to respect patient confidentiality.

Monitoring allows clinicians to get on with their jobs without interruption, indeed it makes it easier for IT departments to implement initiatives like single logins, and to introduce advances like patient portals, as they can make sure that data is secure. If a breach takes place then it can swiftly be tracked to its

[33] For detailed information see www.fairwarning.com/documents/2011-WHITEPAPER-HIE-NHS-SCOTLAND.pdf.
[34] See www.dh.gov.uk/health/2011/08/information-responses/.
[35] See www.medicalprotection.org/uk/booklets/medical-records/confidentiality.

source, ensuring their reputations cannot be tarnished by unfounded suspicions. And ultimately, privacy breach detection provides a powerful defense for the essential relationship of trust that must exist between healthcare professional and patient.

Survey evidence shows that patients see electronic healthcare as important but their confidence would be shaken by privacy breaches: [36]

- *75.5% value electronic records as a way for clinicians to share information and to keep information up to date.*
- *87.3% say that personal data breaches would make them think a hospital was badly managed.*
- *77% believe that chief executives and top managers should do more to stop unauthorised accessing of medical records.*

[36] See *How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* at www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

Patients: My Life, My Record, My Trust

Key Points

- Patients must be able to trust their care teams and hospitals with the most sensitive information about themselves and their children.
- The public expects the NHS to know who is looking at their records – and for those who let them down to be held accountable.
- Patients fear that their families and jobs could be threatened by data breaches.

Care and Trust

Patients appreciate that electronic records are essential to their healthcare – but they firmly believe that their information must be protected in order to keep themselves and their families from harm.

An EU-sponsored survey demonstrated that patients regard medical information as deeply personal. [37] They are also aware of the harmful consequences that could affect them if this information fell into the wrong hands. Survey results from across the UK show that: [38]

- 61% of people are worried that their identity could be used to commit fraud, or by criminals to target them, their family or home.
- 34.1% were worried that sensitive medical or personal information could be leaked to their employer.
- 40% were very or somewhat worried that sensitive medical or personal information could be leaked to people who know them.

These concerns are legitimate and revelations about data breaches are widespread. Stories include: [39]

- The fining of a former Liverpool health worker in 2012 for accessing the records of five members of her ex-husband's family.
- The conviction of a Romford health service employee for unlawfully obtaining her sister-in-law's records to see what medication she was on.
- The discovery that a cleaner in Rotherham accessed a friend's records to see if she had recently had an abortion.

In each case the patients were victimised by the misuse of access to electronic health records and lost control of the most intimate details of their lives. The harm which snooping does is often hard to measure as it can extend from malicious gossip, to the denial of career opportunities or material losses from identity theft or burglary.

Stories such as these can also cut patient's confidence in care providers who, in clinical terms, try to deliver the highest possible standards. For substantial numbers of patients this may already be the

[37] The EU's *Special Eurobarometer 359* report found that 83% of Britons regard medical information as personal (against an EU average of 74%) and 83% trust health institutions to protect their privacy (EU average 78%). For full results see ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[38] See *How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* at www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

[39] See www.ico.gov.uk/news/latest_news/2012/health-worker-convicted-of-obtaining-patient-details-unlawfully-12012012.aspx and www.ico.gov.uk/news/latest_news/2011/receptionist-unlawfully-accessed-sister-in-law-medical-details-16122011.aspx and www.ehi.co.uk/news/acute-care/6549/nhs_trusts_report_unlawful_record_views.

case, with survey results showing that 19.1% of people in the UK have been worried about security of their personal information. [40]

The same survey showed that the NHS is seen as fully responsible for the safety of information, with 97.1% believing that chief executives and top managers have a legal and ethical duty to protect their data. This is entirely in line with the terms of the Care Record Guarantee which says that: 'You have the right to privacy and confidentiality and to expect the NHS to keep confidential information safe and secure'. [41]

In their own words – Patient Advocacy Group

"The future of health services will be built on electronic health records, but if patients don't trust that their medical details will be kept private it could have a catastrophic effect on care. There is a clear need for the NHS to urgently address this issue, as the lax controls put in place by many NHS institutions leave patient records vulnerable to too many prying eyes.

"It is a simple principle that patients should be able to ask who has looked at their medical record, and know that appropriate action will be taken if someone does not respect their privacy. The current system fails patients on both of these points, as the overwhelming majority of abuse will go undiscovered."

Nick Pickles
Director of Privacy and Civil Liberties Campaign Group
Big Brother Watch

Changing Times

With so many new IT supplier entrants to the healthcare market, there is every reason for patients to be concerned that the threat to their privacy could grow. It is also reasonable for them to expect the NHS to live up to its privacy pledges and guarantee that no one is misusing access to their personal data. The NHS Constitution clearly states that; 'you have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure'. [42]

The pressure for action is also being spurred by a growing consensus that patient records are the property of the individual. The NHS Future Forum states that:

- Information is a key enabler of integration. Every individual should own their own patient record and be able to share it as they wish. All care records should be electronic and accessible at the point of care throughout the whole care journey, regardless of sector or provider. [43]

The NHS cannot afford to allow its reputation for confidentiality to be eroded, otherwise there is the danger that patients will cease to trust clinicians with information about themselves – and parents will be wary, or confused, about what it is safe to say about their children.

A simple solution is available in the form of data breach monitoring. This allows patients to be confident that their information is safe. Likewise it provides a solid foundation for the further expansion of electronic healthcare. This is essential if patients are going to give their consent for providers to hold

---

[40] See *How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* at www.fairwarning.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf.

[41] See www.nigb.nhs.uk/pubs/nhscrg.pdf.

[42] See NHS Choices www.nhs.uk/choiceintheNHS/Rightsandpledges/NHSConstitution/Pages/Overview.aspx). The NHS Connecting for Health security principles can be found at www.connectingforhealth.nhs.uk/systemsandservices/infogov/security.

[43] See *NHS Future Forum recommendations to government – second phase* at www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_132026

information about them, and equally vital if we are to see the expansion of tele-health and tele-care, which will enable care to be delivered in the patient's own home.

In their own words – the Information Commissioner

"The health service holds some of the most sensitive information available. The damage and distress caused by the loss of a patient's medical record is obvious, therefore it is vital that organisations across this sector make sure their data protection practices are adequate."

Dawn Monaghan
Information Commissioner's Office
Strategic Liaison Group Manager for Public Services

Conclusions

Healthcare in the UK is at a tipping point. Resources are limited and demand is growing. The greater use of electronic healthcare is a large part of the solution. But the future of electronic healthcare must be built on firm foundations – that demands data breach monitoring and detection. Healthcare organisations across the world are already taking effective action to introduce software which deals with the problem. In the UK, Scotland is showing the way forward.

Those who are left behind run a series of risks. Foremost is that patients' may suffer personal, professional or criminal consequences if their data is stolen. Their loss of faith in the NHS can also discourage them from seeking help or giving full details of their condition. Beyond this, electronic healthcare systems can only succeed and grow if they have the confidence of clinicians.

Fraud is another major concern, denying much-needed cash to the NHS and stealing from taxpayers. Data breach monitoring helps reveal and deter such practices.

There is a heightened political and public appetite for sanctions to be taken against those who are seen as responsible for privacy breaches. Greater patient rights, harsher penalties and tougher legislation must all be factored into the challenges faced by NHS senior management. It is in the clear interests of all UK healthcare organisations to adopt privacy measures which will protect them, their reputations, their patients and their staff from the severe harm caused by the misuse of patient records.

The FairWarning® Solution

FairWarning® invented and is the global leader in privacy breach detection solutions for electronic health records (EHRs). Its systems protect nearly 900 hospitals and 2,600 clinics in the UK, USA, Canada and France. In March 2011, FairWarning® received the contract to provide privacy monitoring software to every health board in Scotland, which will soon have an HIE capable of exchanging data on five million patients.

FairWarning® protects institutions and patients against damaging insider incidents. Privacy monitoring automatically, centrally and un-intrusively reviews and audits usage patterns in EHRs to identify snooping, identity theft, medical identity theft as well as noncompliance issues. Based on referenced FairWarning® customer studies, manual review processes are reduced by over 90% and incident visibility is improved by over 80%.

FairWarning® dovetails with existing privacy processes and leverages the best practices of many healthcare organisations. By automating intensely manual processes, privacy protection provides a positive ROI.

For more information about FairWarning® Privacy breach Detection solutions, please contact UK@FairWarning.com or call (in UK) 0800 047 0933, (in US) 001 727 576 6700.