FORBIDDEN CLICKS

HOW TO SPOT STAFF MISUSING ACCESS TO PATIENT DATA
New powers have just been granted to the Information Commissioner’s Office to conduct compulsory audits on how the NHS handles patient data security.

The move reflects the increased risk of breaches involved in the shift from paper to electronic records, and the widespread sharing of sensitive information between disparate organisations and care teams.

While it tends to be tales of lost computers and memory sticks that hit the headlines, the real issue is often about staff accessing records they have no right to see.

For example, a Newcastle nurse was recently dismissed after accessing patient records and discussing them on social media and earlier cases include one of an IT worker accessing records of female family, friends and colleagues more than 400 times.

For NHS managers this type of incident represents a major legal, ethical, reputational and practical challenge.

In Wales, the NHS is responding by creating the National Intelligent Integrated Audit System (NIIAS).

Darren Lloyd, NHS Wales Informatics Service head of information governance, says it represents a huge advance by providing “a range of automatically generated reports, designed to meet the needs of our local health boards and trusts, instantly identifying any potential issues when access has not been legitimate.”

An indication of the seriousness of the problem is that in November 2014 the Information Commissioner’s Office (ICO) for England recorded 195 health sector data breaches over the previous year – next highest was local government with 55.

This is likely to be a small fraction of the actual privacy breaches and advanced measures will be needed for the NHS to truly come to grips with the issue at hand.

The £750,000 privacy breach contract for Wales was won by Maxwell Stanley Consulting, which will use a system called Patient Data Protect (powered by VigilancePro) to provide the bedrock for NIIAS.

The change it brings is not just about the huge increase in checks that can be carried out in what is monitored.

A sophisticated series of triangulations, drawing from a range of healthcare applications across Wales, can spot all kinds of patterns – such as whether someone is accessing data about their relatives or colleagues.

Maxwell Stanley managing director Martin Gladding says: “Currently there are manual systems in place but these only review a sample and will tend to look at whether people accessing data have the right to do so – this largely misses the point as people misusing data often do have access rights. The question is about what data they are accessing and whether it is being used legitimately.”

Frequently, the issue has more to do with misplaced curiosity than malice, and monitoring provides the chance to improve training.

In dealing with issues of such sensitivity, it is crucial that any monitoring is correct –

Big Brother Watch says NHS breaches led to at least 61 resignations from 2011-14.

With so much potential for disciplinary and court cases, the IT has to provide an irrefutable audit trail and workstreams need to be in place so employers can, at every stage, show the matter was handled properly.

Electronic data capture from multiple sources is valuable for other purposes too. In Wales it will become far easier to deal with many Data Protection Act requests, such as ones from patients wanting to see everything recorded about them over a long period.

Mark Pearse, head of contracts and information assurance at King’s College Hospital Foundation Trust, has worked with Maxwell Stanley on an online PbR (Payment by Results) Assurance project.

He emphasises that: “Significant operational and administrative gains are achieved by electronic data capture. It can easily be translated for many uses, and makes review and audit significantly easier.

“By removing the need to translate the record into an electronic format, it frees up resource to focus on the service they are providing and using that data as powerful business intelligence to effect change.”

Wales is pioneering systems to discourage staff from misusing access to patient data. By Matthew Shelley
Darren Lloyd on privacy

Modern healthcare needs information to be instantly available where and when it’s needed. At the same time it’s essential that patients’ confidential and sensitive information remains secure.

As NHS Wales reshapes healthcare delivery, better information sharing through digital services has become increasingly important, supporting the reform of acute services and increased care in the community setting.

Our national digital services now facilitate the process of electronic referrals between primary and secondary care, making a summary healthcare record available across Wales. Test results, X-rays and imaging will also be available in the near future, with documents to follow in the medium term. This will allow patient information to cross traditional organisational boundaries and make it available wherever the patient receives care.

Electronic sharing of information has augmented the need to uphold the NHS standard of patient confidentiality and privacy. So, the Wales Information Governance Board committed to procuring a new solution to develop a national auditing approach.

This commitment has led us to forming a partnership between NHS Wales and healthcare consultants Maxwell Stanley Consulting to deliver what will be known as the National Intelligent Integrated Audit System (NIIAS). It will advance NHS Wales organisations from their reactive auditing capability into a proactive and more comprehensive process.

We have successfully completed the initial phase of deployment, working closely with Maxwell Stanley to manage complex integrations with existing national electronic health record systems. The solution delivers a range of automatically generated reports, designed to meet the needs of our local health boards and trusts, instantly identifying when access may not have been legitimate to the care of the patient.

Our partnership with Maxwell Stanley, across a five year contract, allows us to “plug in” any newly introduced applications, ensuring that NIIAS is aligned with future developments in the capturing and sharing of patient information.

NIIAS will ensure that protecting patient information remains our principal objective.

Darren Lloyd is head of information governance at the NHS Wales Informatics Service.

And effecting change is seen as vital in a pressured NHS – whether it’s for improving payments, patient records or security, or, indeed, for meeting regulators’ demands.

The ICO, which has issued fines totalling £1.3m to NHS organisations, welcomed February’s new measures which allow it to assess data protection in England’s GP surgeries, NHS trusts and community healthcare councils, and their equivalents in Scotland, Wales and Northern Ireland.

Christopher Graham, the information commissioner, said: “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 is a major cause for concern.

Poor procedures and training

“Time and time again we see data breaches caused by poor procedures and insufficient training. It simply isn’t good enough.

“We fine these organisations when they get it wrong, but this new power to force our way into the worst performing parts of the health sector will give us a chance to act before a breach happens. It’s a reassuring step for patients.”

While there might still be a long way to go, technology available today is capable of addressing many of the challenges facing health bodies and others.

According to Mr Gladding, Patient Data Protect has the ability to see inside emails and detect whether sensitive information is being sent inappropriately – and then flag up a warning asking if the sender is sure they want to go ahead.

Security software can also be linked to CCTV so if a breach takes place it’s possible, for example, to check whether whoever was logged into the computer was actually using it at the time.

At stake in all this is public confidence, which Mr Gladding says has come under significant pressure from data breaches.

“We are moving into an electronic world and this is bringing huge improvements from data breaches.

“But patients need confidence that their data is being monitored and protected in a way they can trust,” he says.

“While NHS organisations are moving forward in electronic healthcare every day, they must also show that patient confidentiality has not been forgotten.”

Protecting patient information remains our principal objective

This commitment has led us to forming a partnership between NHS Wales and healthcare consultants Maxwell Stanley Consulting to deliver what will be known as the National Intelligent Integrated Audit System (NIIAS). It will advance NHS Wales organisations from their reactive auditing capability into a proactive and more comprehensive process.

We have successfully completed the initial phase of deployment, working closely with Maxwell Stanley to manage complex integrations with existing national electronic health record systems. The solution delivers a range of automatically generated reports, designed to meet the needs of our local health boards and trusts, instantly identifying when access may not have been legitimate to the care of the patient.

Our partnership with Maxwell Stanley, across a five year contract, allows us to “plug in” any newly introduced applications, ensuring that NIIAS is aligned with future developments in the capturing and sharing of patient information.

The implementation of NIIAS will add an extra layer of security to the high level of data protection procedures already in use, in addition to establishing a standardised and more effective approach to auditing.

NIIAS will ensure that protecting patient information remains our principal objective. Darren Lloyd is head of information governance at the NHS Wales Informatics Service.