HealthManagement
Promoting Management and Leadership

Volume 5 / Issue 5 / 2010 - Features

Promoting Patient Data Safety With No Headaches

Good information governance is a particularly important area for the healthcare profession where large amounts of personal information about employees and patients are handled every day. Ensuring that access to patient data is secure while also ensuring its availability for relevant clinicians and managers, is critical.Nevertheless, it seems that information security at this fundamental level of access presents serious difficulties for many healthcare organisations.

Author

David Mount,

Technical Director,

NetIQ

Take the example of the UK National Health Service (NHS). Earlier this year, the country's guardian of information protection, the Information Commissioner's Office (ICO) criticised NHS organisations for a range of serious information breaches and mishaps with patient data. In fact, the ICO stated that a quarter of all 250 reported data breaches involved NHS hospitals.

Less Malice than Mistake

It is interesting to look at what lies at the heart of these examples of poor data security. Typically the security problems arise from mistakes rather than malice, such as an Excel spreadsheet of medical records is emailed to another department with no password protection, or passwords being casually shared among staff. The examples tend to appear minor though the potential for serious breaches is considerable.

There is also real scope for regulatory authorities to issue a stiff fine and inflict a damaging blow to a hospital's good reputation.

Information Governance and Regulatory Compliance

Information governance is therefore becoming a compliance issue for healthcare IT professionals. In the case of the UK, the Information Governance Statement of Compliance (IGSoC) was developed by NHS Connecting for Health (NHS CFH) to deal with key information governance issues and to provide a tool to support its responsibilities as a data controller. The requirements for improvements in information security are being ratcheted up, for example, a new level of IGSoC sets a tougher regime for NHS organisations and requires even deeper changes to how patient data is properly handled and protected.

The Need for Simple but Robust Policies

Adhering to these changing regulatory regimes can be daunting, but, the starting point for good IT security within the healthcare sector really starts with getting simple and solid procedures and policies in place.

Arguably, good IT security begins with knowing where your data is stored. Statistics suggest that most data loss actually occurs directly from relational databases. Therefore, protecting the content of these repositories is the first layer in a multi- step process. Having the ability to report in real-time on who is doing what within your environment is a powerful way of managing this risk.

Security and Housekeeping

However, secured data does still need to be accessed by the right people. This is often managed with directory programmes like the ubiquitous Microsoft Active Directory that are the central repository for IT organisations. Active Directory holds critical data on every user, their access privileges and their individual profiles that must be carefully managed.

IT organisations find managing Active Directory extremely challenging because it is a huge and complex administrative burden. The root of the problem is that the programme's own management tools don't give the detailed level of control necessary. This contributes to a general problem with house-keeping of user access rights and creation of rules, especially those associated with groups. The result is Active Directory can

become a weak point in a healthcare organisation's information governance.

Security and House Cleaning

It is not uncommon that the number of groups in Active Directory gets unmanageable. IT organisations are presented with a dilemma. The job of cleaning up these empty or stale groups becomes more and more difficult because deleting a group may break or block access of users to mission critical applications. So it can be less of a risk to leave the "unknown" groups out there than delete them, despite the potential security risk or compliance breach.

The ideal solution would be having in place a defined process for managing a group's lifecycle. Groups should be reviewed and signed off by the business owners to maintain compliance, security or just to keep the directory clean.

Admin controlled and shared accounts can cause major issues when it comes to effective auditing as they are often not linked to specific individuals. Controlling access is only worthwhile if there is clear authentication in place to identify the user and establish that they are authorised to perform these actions on the system. Detailed user activity and log analysis is needed, as is clear segregation of duty to prevent access creep.

Improved Identity and Access Management Tools

IT administrators need to take advantage of tools that can monitor for configuration creep and can help organisations manage privileged users. However, to be useful, the output of these tools needs to be easy to understand. This enables non-IT literate people to have visibility of when and where data is accessed and what changes have been made to the system.

Having better identity and access management systems and policies in place is only half the battle. The critical issue that must be overcome is that when a policy is put in place it has to be accepted by the individuals – the clinicians, managers – it relates to. And, as case studies of good information governance procedures being by-passed indicate, it is not good enough to have an excellent security policy if you cannot assure patients and the regulators that this is understood and applied by everyone, everywhere, all the time.

Of Policy and Complexity

In other words, security policy management and enforcement is the toughest challenge facing IT administrators. The typical sequence of events starts with a policy being circulated to all the relevant people. With more complex policies, a training course will often be carried out.

However, at the end of this process, there is no assurance that the policies are being followed and that they have been interpreted correctly. There is a need to ensure that the policy is understood, such as brief questionnaires that the users must answer correctly to signify their acceptance of the policy and regular checks to make sure it is still being followed further down the line.

This compliance requirement risks adding another administrative layer of checks to be managed and implemented.

The real requirement is for an approach that makes the policy controls entirely systematic and seamlessly part of how

staff manage information in step with strict data protection requirements.

The Promise of Automation

This is an opportunity for IT professionals to consider how security policy management procedures can be automated and thus applied more rigorously. Healthcare organisations can ensure that whenever they have policy in place relating to IT, for example access to the internet, they can tie this in with an automated process to manage the human interaction.

Initially it will re-direct the user to the policy centre like NetIQ VigilEnt Policy Center, presenting them with the relevant policy document that they need to review and accept. It will then test them to ensure they understand the policy before allowing them access to the internet. As soon as this process has been completed once, the system will recognise this and then provision access the internet to that user moving forward. It will then only re-direct the user to the policy centre when there are changes in the policy. Essentially this means that the organisation is now using technology to extend the people side of its business into the process side.

By automating many of the processes associated with data management, the focus can be shifted away from the IT department. By ensuring that key information is automatically processed and the output is produced in non-IT specific language, users at all levels can effectively interpret information and act on it. This helps to reduce bottlenecks that can be caused by over-reliance on the IT department.

An example of this in action would be when a user is due to be granted administrator or root level access privileges. This level of access gives the user the potential to use and edit large amounts of sensitive and system critical data. Automation can be used to gather information to support, or advise against, this level of access for the user. Information including helpdesk tickets, case control, and configuration management can be collected easily and used to send a query to the owner of this data to check they are happy for the new user to be granted access.

Automating security policies can have very concrete returns for healthcare IT organisations. This can apply to being able to better respond to audit regimes, avoid penalties without a heavy expenditure of resources and even make efficiency gains. Demonstrating that patient data is safely handled can have financial rewards such as reducing insurance premiums for litigation protection.

The key for managing these IT security processes and being ready for the health information governance auditors comes down to automation. And the regimes proposed are getting tougher every year. With organisations required to show that their users not only understand and accept key policies, but also demonstrate continued improvement, without bringing automation into the mix this is a near impossible task.

Published on : Thu, 30 Dec 2010