Realtime
publishers
"Leading the Conversation"

The Essentials Series: The Business Imperatives of Compliance in the UK

Managing Compliance in the Healthcare Industry

by Kevin Beaver

Copyright Statement

Managing Compliance in the Healthcare Industry

Until recently, the healthcare industry has had little regulation regarding the protection of patient information. With the transition to electronic medical records, Internet-based patient management and collaboration solutions, and the demand for patient privacy, managers in the National Health Service (NHS), Strategic Health Authorities (SHAs), and Approved Service Recipients (ASRs) have seen a growing number of requirements for keeping healthcare records under wraps. As a result, compliance is no longer optional.

Just how do healthcare managers in the UK approach the challenges of governance whilst maintaining a realistic balance of information risk against the associated costs? Simply put, they have to think about compliance in a new way. It is not a one-time grade or status. Rather, compliance is about changing perception of information risks and adjusting past ways of looking at policy and procedure management.

With the growing number of reports on the loss of healthcare records, something has to change. The old ways of managing patient information are obviously not working. As experience has taught, however, making changes will undoubtedly increase the likelihood of problems. Employees working for healthcare organisations often lack the right knowledge and end up misunderstanding the rules. In addition, there are often cultural and personality barriers among healthcare professionals, making the process more difficult. With this, errors and oversights tend to occur, putting the very essence of compliance at risk. Minimising trouble and ensuring compliance long term can only be done by proactively managing these changes.

Healthcare Governance Imperatives in the UK

In 2008, NHS Chief Executive David Nicholson issued a memorandum to NHS organisations regarding the latest NHS Information Governance Toolkit and information security and privacy compliance requirements. Chief Executive Nicholson said:

> *…we cannot be complacent and continued action is necessary to ensure the adequacy of our systems, procedures, and working practices.*

He went on to say that all SHAs should consider an independent audit of their information governance standards associated with the NHS CFH Information Governance Statement of Compliance version 6. Furthermore, all NHS organisations must:

- Include details of incidents involving data loss or confidentiality breach in their annual reports;
- Make specific reference to information governance in terms of identifying and managing information risks in their annual Statement of Internal Controls;
- Identify a Senior Information Risk Owner at the Board level.

Furthermore, according to the NHS Information Governance Statement of Compliance, ASRs must:

> *…have policies, standards, procedures and systems in place to ensure that they comply with all relevant UK and European legislation and be able to provide evidence, where appropriate, on demand.*

In addition to the NHS directives, other UK regulations affecting the privacy and security of patient information are The Common Law of Confidentiality, The Data Protection Act 1998 and The Human Rights Act 1998. Even with well thought-out compliance documentation, healthcare organisations still have to ensure that the right policies and procedures are properly managed on a consistent basis. This has proved to be the sticking point for many organisations.

The Realities of Transacting with the NHS and the Information Governance Statement of Compliance Requirements

Even with the specific mandates—as with any set of information security regulations, standards frameworks, or best practices—healthcare organisations do have to take into account the following:

- Tangible costs of initial compliance;
- Internal resources required for ongoing oversight;
- If and how the requirements of all applicable regulations across the board can be managed at once at the same level using the same policies and similar procedures

That said, if healthcare organisations are going to transact in today's electronic marketplace, they have to work within the parameters of these regulations. Again, compliance is not optional. How you go about implementing it and managing it will determine how simple or difficult it will be.

The Value of Policies and Procedures in Healthcare Organisations

It's one thing to have well-documented policies and procedures, but demonstrating compliance at any given time is something quite different. Healthcare managers must have the tools and processes for evidencing compliance on demand. This means being able to demonstrate that users are aware of current requirements and processes, and specifically what they have agreed to.

When it comes to compliance, the following are the benefits of sound policies and procedures in a healthcare setting:

- They clearly specify what can or cannot be done.
- They assist with overall information governance and minimising patient and business risks.
- They set expectations of everyone involved, which helps ensure that everyone is approaching things in the same way and sets up all parties for success.
- They spell out exactly what to do and what not to do, which in turn minimises the chances of errors and oversights in daily work.
- They can serve as proof that employees were aware and agreed to the terms in the event that a violation does occur.
- They demonstrate to regulators and patients that the organisation is serious about compliance.
- They help all business units across the organisation by cutting down on duplicated efforts and ongoing administration, which in turn lowers overall costs.

Policy and procedure documentation not only provides multiple benefits to the organisation, it is the only way to manage sensitive patient records safely and securely. The bottom line is that compliance-related directives and rules not documented are merely dreams and unfulfilled ideas.

Security Policy Considerations for the Healthcare Industry

As in most other businesses, many managers in healthcare organisations often do not understand the information risks and compliance concerns that the organisation is up against. There are also managers who assume that just because employees passed a background check and are good workers that they are always going to do the right things. These are dangerous assumptions that often get healthcare organisations into trouble quickly. In my information security work, I see many healthcare organisations failing to adequately implement their policies and procedures. They are often on paper but rarely executed well due to the inherent administrative burden associated with traditional processes. In addition, I often see a general lack of communication between IT, compliance and management, and thus a lot of wasted effort that only serves to create compliance gaps. There are also the cultural and political issues with doctors not wanting to be told how to do their work.

Many people fail to realise the fact that policies and procedures are critical for getting everyone on board and sticking to best practice. This documentation is intended to shape and change behaviour as it relates to handling sensitive healthcare information and basically outlines ‘This is how we do it here’. Unfortunately, policies and procedures are often not used in the way they should be, which ends up creating information risks rather than eliminating them.

It is important to remember the following when putting together compliance-related documentation in an healthcare organisation:

- The complexities of healthcare information systems, business processes, and people often make policies more difficult to enforce.
- An annual review of all documentation is critical to ensure it is still appropriate and applicable.
- Where possible, tie compliance into employee reviews to give people an incentive to follow them.
- Not all policies are alike. Some are mandatory and absolutely critical. Others may not be critical for the protection of sensitive healthcare records. Therefore, it is important to use discretion with enforcement.
- Focus on rewarding good behaviour rather than punishing bad behaviour.
- Establish an audit trail that proves delivery of the policies and procedures to everyone involved, monitors their comprehension, and tracks their acceptance and agreement of each policy.

An integrated information governance and assurance program—supported by management—must be in place to ensure reasonable compliance with the NHS and other regulations affecting the healthcare industry.

Getting the Word Out to Users

A key concern in healthcare is determining the best way to ensure that employees are aware of all the compliance-related policies and procedures. This is especially important in healthcare organisations where timing is critical. Healthcare employees can rarely afford to take time off from treating patients for policy review and training. In order to ensure that employees understand what is expected of them as efficiently as possible, there first must be central coordination via representatives from HR, Audit, or Compliance teams and facilitated by IT. This will help to ensure consistency and simplify communications across the organisation. To help with the process, a centralised and automated system should be used, which can help to provide insight into policy viewing, comprehension and enforcement. That is really the only way to make this work without incurring significant administration overhead.

Always remember that getting the word out one time is not enough. The secret is to get the word out and keep it out by periodically reminding individuals of compliance concepts and their responsibilities when handling patient information.

Essential Requirements for Effective Information Assurance in the Healthcare Industry

With all the complexities associated with the information systems and business processes in healthcare, management has to be extra vigilant to ensure compliance with all the regulations. This often requires previously unallocated resources, but it still has to be done. In fact, Chief Executive Nicholson acknowledged in his 2008 NHS memorandum that the NHS mandates *"require a significant investment of time and energy but we must ensure that the public has, and can continue to have, confidence in our systems, procedures, and working practices."*

Healthcare managers must be aware that just because their organisation is compliant with one regulation, that does not mean it is compliant with all the others. By the same token, compliance does not always mean that sensitive healthcare information is safe and sound and vice versa.

In order to maintain the checks and balances required for information assurance and compliance in the healthcare industry, organisations must have streamlined procedures and utilise automated controls wherever possible. This will ensure that sustainable and repeatable processes are in place. It will also help to provide strong audit trails that prove delivery of the policies and procedures to everyone involved, monitor their comprehension, and track their acceptance and agreement of the applicable rules.

Compliance with the NHS regulations among others starts with senior management, gets monitored by line managers, and ends with users. Minimising costs, maximising effectiveness and proving ongoing compliance in a reasonable fashion can be accomplished. It is just a matter of choosing the right tools for the job and management ensuring that protecting patient information is getting the attention it needs.