

# Legal Admissibility and Evidential Weight of Information Stored Electronically—What are the benefits of implementing the Code of Practice?

*By Alan Shipman*

## History

In the mid 1990s, vendors and users of electronic document management (EDM) systems were concerned about the issue of legal admissibility of electronically stored information. The burning question was—do we need to keep original paper documents? In order to address this issue, those involved in the technology drafted a Code of Practice, detailing policies and procedures that would enable users to demonstrate the authenticity of electronically stored information. This Code of Practice was published by the British Standards Institution (BSI) in 1996, as BSI DISC PD 0008.

The 1996 Code was based around Write Once Read Many (WORM) storage. At the time, WORM optical disk was the major storage medium used in EDM systems. There was also the issue of being able to demonstrate that electronically stored information had not been changed during its storage life. It was known that information stored on computer systems could easily be corrupted, hacked into or otherwise accidentally or maliciously changed. The use of a storage medium that builds in automatic protection gave a high degree of confidence to users of such systems.

During the later part of the 1990s, magnetic disk systems and rewritable optical disk technology became the normal storage media used by EDM systems. Some media manufacturers gave users the WORM confidence by including within the storage systems (often as firmware) the ability to turn on WORM protection, thus being able to comply with the requirements of the 1996 Code.

The second version of the Code of Practice was published in 1999. The scope of the Code was extended to include all types of storage media, whether WORM or rewritable. The Code noted that additional protection is required where non-WORM storage is used. This version of the Code also included numerous improvements, especially where the technology used in EDM systems had moved forward.

The third version of the Code of Practice has now been published, as BSI BIP 0008:2004. The text has undergone significant review, to assist in the understanding of the compliance requirements, and in the addition of examples of typical implementations. Some areas have been updated from a technical standpoint, where improvements or enhancements in EDM systems have been made. This version also recognises the recent publication of ISO/TR 15801, an international technical report based on the 1998 version of the Code.

## Benefits of compliance

So, what are the benefits in implementing the requirements of the Code of Practice? It is reported that many hundreds of organisations, in both the public and private sectors, have implemented the Code, although no official statistics are available to confirm this. These organisations must be gaining significant business benefits from compliance with its requirements in order to be able to continue to justify the efforts required.

The implementation of ‘best practice’ in electronic document management, as defined by the Code of Practice, should achieve many business benefits. Using the experience of the many contributors to the Code should always result in improved systems. Examples of areas where business benefits can be achieved are:

### System reliability

One of the significant advantages in following the recommendations in the Code of Practice is that all appropriate policy, security, procedural, technical and audit issues will have been identified. Appropriate measures will be put in place to manage these issues, as is relevant to the application concerned. This should have a positive impact on reliability, both in terms of system availability time and on information accuracy.

### Original document destruction

The major risk undertaken when destroying original documents subsequent to their being scanned and stored on an EDM system is the potential of a challenge to the authenticity of the electronic 'copy'. Where copies of documents are used as evidence in court (or in any other circumstance), it may be necessary to be able to demonstrate their authenticity. The recommendations contained in the Code of Practice are designed to make this proof of authenticity straightforward to achieve.

There are many advantages in not storing original paper documents, where electronic copies exist, such as:

- saving of storage space, including buildings, power, heating, security, etc.
- saving of storage equipment, such as filing cabinets, cupboards, boxes
- saving of staff who manage the filing and indexing of the paper files
- saving of staff involved in locating and retrieving original documents
- where original documents are stored with third parties, saving of storage and retrieval costs.

### Safeguarding evidential value

Most business documents contain evidence of an agreement, business process or other activity. Typically, it is not known whether the evidence contained in a particular document will be crucial in resolving a future dispute. Thus, it is important for organisations to store their documents in such a way that the evidence contained in them is retained for as long as is necessary.

In order to safeguard evidential value, two issues need to be addressed, both of which will be achieved when implementing the Code of Practice, namely:

- ensuring that all relevant evidence is captured from original documents, including metadata
- being able to retain the evidence during storage.

### Improved access

Keeping documents in an electronic form in an effective EDM system will result in improved access to the stored information. By ensuring that the appropriate indexing and search facilities are available, as well as the necessary access rights to the information, efficient retrieval will result. Again, these are issues dealt with in the Code of Practice.

### Improved security

One of the key elements of the Code of Practice is that appropriate security measures are implemented, and are reviewed at regular intervals. It is also essential to have a documented procedure to follow should a security breach occur (or be suspected). By requiring appropriate security policies to be developed and implemented, EDM systems will be operated in a secure manner, a vital fact which will contribute to any proof of authenticity requirements.

### Reduced costs

By managing EDM systems in accordance with best practice guidelines, expensive mistakes in process design should be avoided. This, combined with the cost reduction that can be achieved by not storing original paper documents, should reduce the overall cost of document management within the organisation.

### Reduced document handling

Another process that is included in the detail of the Code of Practice is the management of originals during their electronic storage. An example of where business efficiencies can be gained is the handling of original documents after storage on the EDM system. The improvements in system reliability (see above) gained often allows the originals to be kept away from the 'real' business areas. Where paper originals are concerned, organisations which can demonstrate compliance with the recommendations of the Code will simply box up the originals after scanning, and destroy them after a short time.

### Improved awareness

Where the Code of Practice is implemented, users are more likely to be aware of the value of the documents stored on the system. This is ensured by the need for formal documented procedures in all areas, which are designed to protect the integrity, and thus the authenticity, of the stored documents.

### Improved quality

As already noted, ensuring that the evidential value of the stored document is not compromised, appropriate quality management procedures need to be implemented. These procedures include the quality control of document scanning systems as well as the quality of the procedures being used.

### Private and public sectors

With the increasing need for reliable and cost-effective document management, in both the private and public sectors, compliance with the recommendations of the Code of Practice is becoming increasingly necessary.

#### Private sector

Effective document management is key to business efficiency and competitiveness. The value of an organisation's information asset is seen as critical in many business sectors. The Code of Practice is not aimed at any business sector in particular—indeed it is being implemented in all sectors.

The pharmaceutical industry is using the Code to protect the integrity of its drug development and testing information, where the loss of a particular piece of information could be very expensive. The finance industry is storing vast numbers of documents electronically and reaping the rewards of reduced storage costs, etc. Again, they are implementing the Code of Practice to safeguard the integrity of their stored information.

#### Public sector

One of the major drivers for effective document management in the public sector is the imminent implementation date for the Freedom of Information Act 2000. By January 2005, all public sector bodies (and there are in excess of 80,000 of these in the UK) need to be able to supply within 20 working days, copies of the information requested.

As part of the guidance developed to assist in the implementation of the FOI Act, the Lord Chancellor's Department (now the Department for Constitutional Affairs) has issued a Records Management Code of Practice (the 'Section 46 Code'). This Code states:

*Authorities should seek to conform to the provisions of BSI DISC PD 0008—A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (2nd edition)—especially for those records likely to be required as evidence.*

This is a direct requirement for all public bodies to implement the Code of Practice.

There is also guidance from The National Archives (formerly the PRO). They provide standards and guidance on all aspects of records management. This includes a set of functional requirements for records management systems, which mainly focus on the technical issues. These requirements include a recommendation to comply with the BSI Code of Practice.

### Records management issues

Since the publication of the 1999 version of the Code of Practice, many organisations have begun using the new international standard on records management (BS ISO 15489)<sup>1</sup>. As there is a substantial overlap in the area of applicability between the Code of Practice and this guidance on records management, one of the major requirements of the 2004 revision was to ensure that the two documents could be implemented in tandem.

#### Use of BS ISO 15489

In order to ensure that all the relevant controls included in BS ISO 15489 were also included in the Code of Practice, one of the actions undertaken during the 2004 revision process was to analyse the records management standard clause by clause, identifying each recommendation. Each of these was then cross-referred to similar controls in the Code of Practice.

#### Mapping to BS ISO 15489

An annex has been included in the 2004 Code of Practice, mapping the content of the records management standard to the Code of Practice. This mapping allows the two documents to be implemented in tandem without any conflict and with a minimum of effort.

## Content of the Code of Practice

The Code of Practice is structured in five parts, as identified in BSI PD 0010:1997 *Principles of Good Practice for Information Management*. Each part needs special attention if the benefits identified above are to be maximised.

### Information management policy

Does your organisation have a policy for managing its information? In the past, such a policy has been relatively straightforward to produce and authorise, as it was simply a matter of a retention schedule. Most organisations—but not all—have such a schedule.

However, there is an increasing choice of media upon which electronic information can be stored (CD, DVD, WORM, rewritable optical disk, magnetic disk, magnetic tape to name a few). The Code recommends that a document management policy is developed, expanding on the retention schedule to include such details as media type, file format, destruction policy and responsibilities.

### Duty of Care

Does your organisation have an Information Security Policy? When the value (including the cost of recovery from loss) of your organisation's information is assessed, it is soon evident that such a policy is essential. It is worth noting that, for most organisations—large and small alike—loss of a significant part of their information may result in loss of business. Either you do not know what to do (loss of information) or people will not trade with you (loss of image).

Has an unauthorised person seen your information, such that your business secrets are no longer secret?

Can you trust the information you store electronically—or has a virus attacked it and changed it, without you knowing?

Can you retrieve your information when you need it?

These three topics (confidentiality, integrity and availability) need to be reviewed, often in consultation with IT departments, to maximise confidence in your systems. Can you trust the information stored in them—even after storage for many years!

### Procedures and processes

So, your electronic storage system has been installed. How do you use it? What procedures will you need to implement? What applications will it be used for?

Compliance with the requirements of the Code of Practice depends heavily on the availability of procedural documentation. Procedures will include preparation of paper documents, scanning, indexing and retrieval. There may also be importing document files from other systems, producing output for court, system backup, operator maintenance and security procedures.

The Code of Practice takes you through all the appropriate procedures that you may need to implement and suggests a number of issues to consider whilst defining them.

### Enabling technologies

The Code of Practice details the EDM system requirements necessary for compliance. Such topics as access control, media storage, system integrity, image processing and image compression are discussed. As with procedures, the technology needs to be documented.

Another topic discussed in this section is the potential need for migration. EDM systems have a relatively short life, being replaced by newer, cheaper and faster systems. Typically, systems will be replaced at approximately five-year intervals. The Code of Practice includes the requirements for successful migration, to ensure that authenticity is not compromised during such an operation.

### Audit trails

This is the area most frequently forgotten by users and suppliers alike, but is an area which can prove to be of prime importance.

What happened to a particular document? When did it arrive? Who approved it? When was it deleted? All this information may prove critical if authenticity is challenged.

Also, to use that well known legal phrase: “Was the system working correctly at all material times?” How do you prove this if you do not know what happened to the technology, when it happened and how errors were corrected?

The Code of Practice recommends the keeping of fault reports, transaction logs, scanning records, etc. There is also the issue of retention periods. If documents are kept for, say, seven years, then it is likely that you will need to keep audit information for seven years also.

But, audit trail information (particularly with workflow systems) can be very large, and thus will require a significant amount of computer storage space to hold it. Have you got enough? Do you need to keep everything or can you discard a significant part of what is produced, keeping only what your legal colleagues might need?

### How much effort is needed to comply?

This is always a difficult question, as it depends upon the current status of the EDM system that you either already have or that you plan to implement. If your system has been implemented in accordance with best practice, then it is likely that you will already be compliant. However, in practice, most systems are implemented in isolation and thus may fail to comply in some areas.

To assess the current status of compliance with the requirements of the Code of Practice, BSI also publish a Compliance Workbook (BIP 0009). This Workbook consists of a series of questions, each of which needs to be reviewed and answered. Where a question has a positive answer, then compliance with the relevant point is confirmed. A negative answer means that some work will need to be done. Typically, it takes one to three days to complete the Workbook for the first time. Some investigations may need to be carried out on particular issues, which may lead to more time being needed. There may also be a need to consult with the system supplier, who might themselves need to go back to the original manufacturer or software developer for appropriate answers.

Once the Workbook has been completed, a project plan can be developed to address the non-compliance points. In some cases, based on a risk assessment comparing the cost of developing a correction with the likelihood of the particular issue being identified as a potential cause for the loss of authenticity, a non-compliance point might not be addressed. This project plan should indicate the resource requirements to achieve compliance.

In typical cases, most of the compliance points are addressed by implemented systems. Compliance points that are often found to be missing from systems are:

- no Information Policy document
- no retention schedule
- inappropriate security controls
- lack of procedural documentation
- insufficient control on document input procedures
- insufficient information about the technology from the system supplier
- use of inappropriate facilities, such as image clean-up
- no thought of future migration requirements
- lack of documentation on audit trail content and access procedures.

Each of these could potentially compromise the ability to demonstrate the authenticity of the stored documents.

### Conclusion

So the moral of the story is, using the BSI Code of Practice is very likely to help you to achieve the maximum business benefit from the electronic storage of information. In some applications, it is almost essential—so why wait?

*Author: Alan Shipman*

*Alan Shipman is a director of Group 5 Training Limited. He was the editor of the 1996 and 1999 versions and the author of the 2004 version of the BSI Code of Practice. Alan can be contacted on 01923 450527 or by email at a.shipman@group5.co.uk.*

*The Code of Practice can be obtained from BSI Customer Services (tel: 020 8996 9001). Further information can be obtained from [www.bsi-global.com/informationmanagement](http://www.bsi-global.com/informationmanagement).*

### Reference:

1. BS ISO 15489-1:2001 *Information and documentation. Records management. General*