

Softology Ltd.

**The legal admissibility of information
stored on electronic document
management systems**

July 2014

SOFTOLOGY LIMITED

• www.softology.co.uk

Specialist Expertise in Document Management and Workflow • 01925 438 030

• sales@softology.co.uk

The legal admissibility of information stored on electronic document management systems

British Standards Institution (BSI) BIP0008 - Code of Practice on Legal Admissibility and Evidential Weight of Information Stored Electronically

Introduction

The BSI Code of Practice is concerned with 'the authenticity, integrity and availability of electronically stored information, to the demonstrable levels of certainty required by an organisation. It is particularly applicable where this stored information may be used as evidence in disputes inside and outside the legal system'

ISO 15489 (BS ISO 15489-12001) is the international standard on records management. As there is overlap between the BSI Code of Practice and the International Standard the 2004 revision of the Code of Practice was to ensure that the two documents could be implemented together. The 2004 Code contains an annex mapping the content of the records management International Standard to the Code of Practice. The Code of Practice was originally published in 1996 as BSI DISC PD 0008. It was updated in 1999 as BSI DISC PD 0008:1999. The current Code of Practice is BSI BIP 008:2004.

Overview

The issue of Legal Admissibility is at the core of records management principles. An organisation needs to be able to prove (to a court of law or some other statutory body) that the contents of a particular document or data file created or existing within an Electronic Document Management System have not changed since the time of storage. If the data file is an electronically stored image of an original paper document, an organisation must be able to prove that the electronic image is a true representation of the original. Proving the authenticity of electronically stored documents is crucial to their admissibility in a court.

In England and Wales, the main statute governing the admissibility of documents is the Civil Evidence Act 1995. This Act resolved many of the outstanding legal difficulties that had arisen through the use of computers for information storage. The Civil Evidence Act shifted the argument from legal admissibility to evidential weight or value. It makes it easier to prove the authenticity of documents, by producing the original or a copy, irrespective of the number of removes between the original and the copy and irrespective of whether or not the document is a paper one or an electronic one. The court needs to be satisfied as to the authenticity of the copy, and therefore an organisation needs to be able to demonstrate that it has administrative procedures that will satisfy the court as to a document's authenticity. Irrespective of issues of legal admissibility or evidential weight, an organisation should ensure that the electronic storage of information complies at all times with best practice. As well as needing to meet legal requirements an organisation has business and ethical reasons for ensuring that the information it controls is not mishandled.

An organisation needs to demonstrate that it complies with the five principles of information management on which the Code is based. These principles are encapsulated into a code of practice - the "Code of Practice for Legal Admissibility and Evidential Weight for Information Stored Electronically" (BIP0008) published by the British Standards Institute. Compliance with BIP0008 will ensure that the organisation manages its information according to best practice, thereby maximising the chance of electronic records being satisfactorily authenticated.

An organisation will need to have in place the following five information management components:

1. Representation of Information (i.e. an information management policy)
2. A Duty of Care
3. Business Procedures and Processes
4. Enabling Technologies
5. Audit Trails

1. Representation of Information

An information management policy document will set out, for operating staff and any future litigants, the rules surrounding the various forms in which documents are held, the documents' life cycles and the legal advice sought and acted upon. The policy should set out in as much detail as necessary the variety of documents that will be presented for storage, for example: Internal and external correspondence, reports, drawings and specifications, legal documents and, perhaps, photographs, video and audio files. It will typically describe the different types of information held within the organisation and, for each type, specify:

- The level of security
- Appropriate storage media
- Formats and version control
- Information management standards, e.g. quality
- Retention and destruction policy
- Responsibilities and roles for information management functions
- Responsibilities for compliance with the code BIP0008

Any system needs to be flexible enough to satisfy the requirements of the organisation's information management policy. It must be capable of:

- Meeting the highest security standards set out in the policy
- Integrating with a wide range of storage media
- Handling different document types
- Managing documents under version control
- Meeting the retention requirements
- Meeting information management standards, e.g. storing images to the quality standard set out in the policy
- Allowing documents to be permanently erased

The 2004 Code recommends that a document management policy be developed, expanding on the retention schedule to include such details as media type, file format, destruction policy and responsibilities.

2. Duty of Care

To fulfil its responsibilities under the duty of care principle, an organisation will need to have in place:

- An awareness of the legislative and regulatory bodies pertinent to its industry
- A chain of accountability and defined responsibility for activities involving electronic document management at all levels
- A system to keep up to date with information management theory and practice, and developments among
- Appropriate bodies and organisations
- A documented information security policy

Under the duty of care responsibilities the system must have the functionality to allow for separation of roles. The person who inputs data should not be the same person who performs quality checks. This separation of administrative roles should be able to be mirrored in the logical access controls within the EDM SYSTEM. The British Standard BS 7799: 1999 (ISO 17799) "Code of Practice for Information Security Management" is the UK/European reference document for information security. Proof of compliance with BS 7799 will usually demonstrate that an organisation has exercised a duty of care.

3. Business Procedures and Processes

An organisation should have documented operating procedures (a user manual) for each of the information management systems it runs. The procedure manual is the document that the organisation will produce, if its electronic storage methods are ever challenged, to prove to auditors, lawyers or judges that the processes are precise, secure and approved for its normal business procedures.

The user manual will typically define the following:

- Document types
- Preparation of documents prior to scanning
- Photocopies
- Batch control
- Scanning processes
- Scanning specific documents
- Image Processing
- Compression Techniques
- How information is indexed

- Quality control
- Procedures for producing authenticated output
- Procedures for authenticating copies of documents
- How information is transmitted within the system
- Procedures for document retention and destruction
- System maintenance schedules
- Security and protection, including encryption and the use of digital certificates
- Backup and system recovery procedures
- Use of bureau services
- Workflow
- Date/time stamping
- Version control

It is important for the system to be able to produce output that will ensure that a document is appropriately authenticated.

The Code insists that the procedures and processes be audited annually, or more frequently for legally sensitive archives, to make sure that the approved procedures are being observed or that new ones meet the requirements of the Code and are formally and properly incorporated in the manual

Some specific recommendations in the code include:

- Preparation of documents prior to scanning

The code requires that:

"Documents should be examined prior to the scanning process, to ensure their suitability. Such factors as their physical state (thin paper, creased, stapled, etc.) and the attributes of the information (black and white, colour, tonal range, etc.) should be noted. Procedures for this examination process should be documented in the user manual."

The Scanning Process

The Code requires, for example, that records be kept on the system audit trail of key information concerning imported documents. This information should include as a minimum:

- Unique identifier for each batch of documents
- Date and time of scanning
- Identity of the person who performed the scanning
- Type of material scanned (e.g. paper document, microfilm, aperture card, etc.)
- Number of documents and number of pages in each document scanned
- Detail of post-scanning processes (de-skewing, de-speckling, etc.) performed

The Code recommends that records be kept in batches so it is easier to check that:

- All required activity has been performed
- Any anomalies have been noted
- Appropriate quality procedures have been completed
- Records of any exception processing have been made

These batching recommendations allow a company to acknowledge that its system cannot be perfect, but that it has seen the anomalies and has registered them, either with a view to correcting them or merely making note of them. If the accuracy the system is challenged in court, the company will be able to it knows where mistakes are made.

Indexing

The Code makes the statement:

"Indexing is a vital part of the process of storing documents"

Whether the system involves automatic indexing, manual data entry, or a combination of these, the Code insists that:

"Procedures for indexing documents should be described in the user manual. These procedures should include methods of checking the accuracy of the index records created."

It sets out what should be recorded, what the audit trails should reveal and operator training requirements. It reminds the records management team to set realistic quality control criteria and processes for noting errors and levels of legibility.

Quality Control

It is important to be able to demonstrate to a court that quality controls are adequate and work. The Code sets out several important processes, including these:

"A sample set of original documents, or of documents equivalent in characteristics to the original documents, should be assembled for the purposes of bench-marking scanning system performance against the quality control criteria."

and

"The result of all quality control checks, including Test Target scans, should be recorded in the quality control log."

The records manager must test and check regularly and record the results of those tests and checks.

Document Retention

The Code says that all retention and destruction procedures should be recorded in the user manual. It sets out instances when, even if company policy is to destroy all documents after scanning, some papers may have to be retained:

- Where photocopies have been used to aid the scanning process
- Where the original is of poor quality and below the standard required by your system
- Where an original contains amendments that cannot be identified on a scanned image.

"No original source document should be destroyed until the write processes have been verified and appropriate backup procedures completed."

Originals should not be shredded until it is clear that the scanning and indexing processes have been completed properly and the data has been backed-up.

Security and Protection

Security and protection covers user access, mixed and/or removable media storage, file transfer protocols, data and hardware security, virus infection, power failure and auditing. The Code states:

"Where mixed-media hierarchical storage systems are used, they should be assessed to ensure that they are used in a write-once mode only."

"Data file transfers, such as moving documents from one device to another, should be controlled by the application software. It should not be possible to move documents or change index data without an entry in the audit trail."

"Although the user facilities (document input and output) may be provided in a normal (unprotected) environment, the central part of the system (file servers, data storage, system software, etc.) should be installed in a secure area with restricted physical access."

4. Enabling Technologies

A typical system will be comprised of many different technologies. Each of these technologies, or rather their component parts, will need to comply with BIP0008. The Code describes technologies that may be used in a storage system and how they should be utilised and controlled to ensure that the system will store documents in accordance with BIP0008. These technologies include:

- Storage media
- Access control mechanisms
- System and data integrity
- Image processing
- Compression techniques

- Compound documents
- Data migration
- Document deletion

Each of these properties of an eDM system is critically important.

Storage Media

The issue of appropriate storage media is critical. There are two types of storage media, distinguished by the medium's ability to be written to many times or just once:

- Write many - or 're-writable' technologies
- Write once - commonly referred to as WORM ('write once - read many') technologies

An alternative way of considering data storage technologies is to distinguish between magnetic media and optical media. In general, magnetic media are write-many technologies while optical media may be write-once or write-many. CD-RW (CD re-writable) and erasable optical disks are optical technologies that can be written to many times. It isn't necessary to use WORM technology to comply with BIP0008. While WORM has the advantage that it is not possible to directly modify data once it has been stored, in practice data is modified by deleting the original data and writing the modified data. Each time a file is modified a new copy of the file has to be written, rather than just overwriting the existing file. The available storage space can be reduced much more quickly than expected. As WORM storage is more expensive than magnetic disk (and even RAID array), the use of WORM exclusively for storage can be expensive. Access to data on a WORM drive, particularly one in a jukebox, is slower than access to data stored in a RAID array. Data stored on magnetic disk can in principle be modified. However the risk of this happening, while significant, is small and the risk can be minimised, if not eliminated altogether, by ensuring that adequate controls are implemented in both the storage system and the eDM system access control system. Users with read only access rights cannot modify the data but those with read/write access obviously can, and therefore there is a requirement to securely log at the system level all read/write accesses so that unauthorised writes to the system can be detected.

Access Control

The system must have an adequate access control mechanism implemented so that individuals, groups and roles can be distinguished, and permissions granted based on the access control list.

System and Data Integrity

The system should provide an environment in which the integrity of the data is preserved, including the transfer of data between the eDM system software and the storage medium. Data integrity should be inherent to the eDM system and any integrity anomalies should be automatically detected and reported. Malicious attempts to change the data should be detected, though if the person acting maliciously has sufficient knowledge of the system's

integrity checking mechanism, it might be possible for that person to alter a document and to 'fool' the integrity checking. Digital signature technology ensures that the integrity of a data file or a document in a system can be verified. A document that has been digitally signed cannot be altered without invalidating the signature. The eDM system software should be capable of working with the technology that implements digital signing. The signature also has a secondary role, one of non-repudiation - the person creating a document and signing it cannot subsequently deny authorship.

Compound Documents

A compound document contains a variety of parts - photographs, graphics, text, and video perhaps. It may be disassembled and each part processed in different ways. The Code advises that they be stored on the same storage device along with the metadata needed to identify the respective locations automatically and make an "accurate and unambiguous reconstruction" of the complete document.

Image Processing

Image processing is a post-scanning technique to improve the quality of a scanned document. These processes can include de-skewing, de-speckling, background clean-up, border, "noise" and forms removal. Though there can be good reasons for improving image quality, care must be exercised in image clean-up to ensure that essential detail is not removed. The Code warns that the techniques are used "with extreme care". De-speckling, for instance, carries a high risk of removing punctuation or decimal points. Any image processing should be identified in the system user manual. Any image processing techniques used could reduce the evidential weight of subsequent retrieved images.

Compression Techniques

Systems storing scanned images normally use compression algorithms to reduce file sizes so that storage requirements are reduced and system performance improved. It is important to ensure that images, when compressed, are not subject to data loss. If the compression technique is a 'lossy' one (for example storing an image as a JPEG) then detail necessary to authenticate the stored image may be lost, reducing the evidential weight of the image. If lossy compression is used, a sample set of scanned images should be made to check and approve the level of information loss. Lossy compression should not be used for documents containing primarily text, but may be more acceptable with photographs.

Data Migration

A system should have the ability to migrate documents and data to some to other hardware/software platforms and other storage media. Documents, such as personnel records, may have a lifetime longer than the current system and therefore at some point will need to be migrated. The system should use open or industry standards for data storage rather than proprietary ones.

Document Deletion

To meet the requirements of Privacy or Data Protection Acts, it may be necessary to amend or delete documents, or parts of documents. This might occur routinely, as part of the organisations' retention policy, or exceptionally as a result of legal or regulatory requirements. Note that a WORM ('write-once, read-many') storage medium could make this operation difficult. The Code sets out acceptable methods - use of masks, index entry cancellation, document replacement, etc. – which should be identified in the user manual and whose use must be recorded in the system audit trail. See the "Guide to the Data Protection Act" for further details.

5. Audit Trails

BIP0008 requires that a system must have full auditing functionality. Without detailed audit trails (i.e. a record of a document's life history) authenticating a document, and therefore satisfying a legal body, may not be possible. In addition, irrespective of legal requirements, an organisation will require audit trails to meet its own managerial requirements, such as internal audit. The audit trail, as a minimum, should log details of each significant event in the life of a document in the system.

The audit trail should:

- be generated automatically by the system
- contain date/time stamps for each event
- be non-alterable
- be stored in accordance with the organisation's information management policy
- be subject to appropriate access control
- be securely stored and backed-up

The system should be able to provide an enquirer, with appropriate permissions, (even one unfamiliar with the processes) access to the full audit trail record and, preferably, have a reporting tool to allow production of customised reports from the trail. 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 at least seven years also.

Compliance Workbook (BSI PD0009)

The British Standards Institution Compliance Workbook (PD0009) is available to aid implementation of the Code. Its pages parallel those of the Code, reminding and instructing systems managers what to undertake. All questions have a Yes/No tick box to ensure compliance.

Principles of Good Practice (BSI PD0010)

The Image and Document Management Association (IDMA) Principles of Good Practice for Information Management, PD0010, is published by the British Standards Institution as the third in its "legal set" of guidelines. It is "Intended to help those who have responsibility for assisting their employers to develop and operate new methods ..."