General Practice Information Technology (GPIT) Group

Scanning and Shredding Documents: impact statement

File Name: Scan_Shred_v0_7.pdf
Version number: 0.7
Date: 25/02/2009
Status: impact statement
Authors: GPIT Group
Distribution: public domain

1. Table of Contents

2. Document History

2.1 Document Creation

Date	Version	Authors
13/03/2007	0.1	GPIT project manager, co-ordinator and facilitators
24/04/2007	0.2	Brian O'Mahony
09/01/2008	0.3	Contributions from Dr Brian Meade, Mr John McDonnell, Mr Brendan Murphy & Mr Patrick O'Neill
28/05/2008	0.4	Feedback from Ms Ciara M O'Sullivan (Office of the Data Protection Commissioner)
07/11/2008	0.5	Brian O'Mahony
17/12/2008	0.6	Brian Murphy & Brian O'Mahony
25/02/2009	0.7	Brendan Murphy

2.2 Document Distribution

Date	Version	Distribution
13/03/2007	0.1	GPIT Group
24/04/2007	0.2	Public domain
09/01/2008	0.3	Public domain
28/05/2008	0.4	GPIT Group
07/11/2008	0.5	GPIT Group
25/02/2009	0.7	GPIT Group

3. Request For Comments

In the transition from paper to electronic records the management of scanned documents and in particular the question of whether or not to shred documents is important for health care professionals and patients. This is an impact statement on document scanning and shredding in Irish general practice. We would like to hear your opinions. The GPIT Group is happy to have comments, corrections and feedback on this document.

Please write, fax or email your comments to:

Dr Brian O'Mahony
GPIT Project Manager
Convent Road, Lismore
County Waterford, Ireland
Phone 058 54255, Fax: 058 53474
Email bom@iol.ie

If possible, please indicate the document version number, section and paragraph you are commenting on and propose new wording.

Thank you.

GPIT Co-ordinator
Dr Brian Meade
GPIT Project Manager
Dr Brian O'Mahony
GPIT Facilitators
Dr Donal Buckley: HSE Dublin / Mid Lenister
Dr Fergus McKeagney: HSE Dublin / Mid Lenister
Dr John Cox: HSE Southern Area
Dr Anne Lynott: HSE Dublin / North East
Dr Frank Hill: HSE Southern Area
Dr Kieran Murphy: HSE Southern Area
Dr Jack MacCarthy: HSE Western Area
Dr Barry O'Donovan: HSE Western Area
Dr John Sweeney: HSE Western Area
Dr Martin White: HSE Dublin / North East

4. The Paper Environment

All organisations today operate in a world which is dominated by technology. In the past all patient records were paper, in the future all patient records will be electronic. Right now we are in transition, in what is generally known as a hybrid situation. Our emphasis should be on reducing the number of documents we send and receive in paper format. Major improvements have been achieved in the last five years, particularly in respect of electronic messaging of laboratory results and radiology results. The range and availability of electronic messages needs to be expanded. One type of document, for instance, that continues to be sent in paper format is discharge and outpatient letters from hospitals to general practice and there is certainly potential for digitising this particular process.

In considering how to manage paper records it is important to make the distinction between old and new records. The general practitioner who takes over a practice and finds him or her self in possession of paper records going back many years may decide to scan the records of active patients into the practice management system but would be well advised to keep the old paper records. A practice which is receiving discharge letters on current patients each day, is confident that their handling of scanned documents is robust and follows good practice, can scan and shred such documents.

In relation to scanning generally, data should be accurate, complete and up to date. In the scanning context, this would mean that a practice should satisfy itself that its scanning procedures are robust enough to ensure that the scanned copies are an accurate copy of the manual records, e.g. that patient and health care professional signatures are clearly reproduced in the scanned version.

In relation to the management of scanning, whether it is handled by an outside company who may need to be brought in to handle a mass scanning exercise and the subsequent ongoing scanning taking place in-house, this should be handled by personnel who are subject to strict confidentiality contracts given the amount of sensitive information which they will have access to.

5. The Management Of Scanning

Every practice manages paper differently. Differences include who opens the post, who reviews the documents, who comments on the documents, who actions the documents, how they are stored, how long they are kept and what happens when staff are on holidays. Each practice needs to review their handling of paper, streamline it and agree a practice workflow for scanning.

5.1 Attribution

Each scanned document should be linked to an entry in the patient electronic record. The entry should indicate:

- The date of the original document;
- The nature of the original document, for example: discharge letter, outpatient clinic letter, letter from speech and language therapist, etc.

- The author of the original document, for example: Dr Michael Smith, Consultant Cardiologist:
- The institution of the original document, for example, Department of Cardiology, St Elsewhere's Hospital, Dublin;
- Any note or comment that the doctor or nurse wishes to make about the document;
- The date the document was scanned;
- The identity of the person scanning the document;

The last two items above could be generated by the software system based on the current date and the user log on. To facilitate rapid and efficient capture of the complete attribution information it is necessary for the practice software to provide a user friendly interface.

5.2 Workflow

It is good practice to indicate who has reviewed and acted on a document or report. The following description of a workflow process for review and comment may be useful to GPs and practice software vendors.

All appropriate practice staff should review and comment on the scanned document. One person, normally the general practitioner or practice nurse caring for the patient, should carry out any actions necessary and sign off on the scanned document. The actions required could include:

- Contacting or reviewing the patient:
    - Phone the patient;
    - Schedule an appointment for the patient;
    - Write to the patient;
    - Send an SMS text message to the patient:
- Patient referral:
    - For a consultant opinion;
    - For a diagnostic test;
- Prescription:
    - Issue a prescription;
    - Change medication;

Scanned documents should remain active until one of the general practitioners or a designated practice nurse has signed off on the document. Procedures should be agreed for signing off documents when staff are on leave and for review of documents by staff who return from leave.

In terms of the use of SMS text messages, the practice should get prior agreement from the patient before text messaging is used, and even when this agreement has been obtained, the reference to health information in text message format should be minimised given the potential for third parties to access mobile phones.

6. File Standards

A scanned document is an image or electronic photograph of the original. File types such as Tag Image File Format (TIFF) and Joint Photographic Experts Group (JPEG) are acceptable for image files. Sometimes the process goes a step further and optical character recognition (OCR) is used to convert the image to text. Optical character recognition is not 100% accurate. The gold standard for scanned documents is the image file. OCR without storage of the original image is not acceptable.

Method	Acceptable?
Storage of image file in TIFF or JPEG format	Yes
OCR with no storage of original image	No
OCR with storage of original image file	Yes

Table 1 Acceptable image file standards

The minimum resolution for scanned images is 300 dpi. Higher resolution may be used as necessary to achieve high quality images or for specific image types. While there are no quality standards for images, care should be taken to provide the best quality available from the original. 400-600 dpi resolution is recommended for color and halftone photographs.

7. Audit Trail

The audit trail tracks what happens to the electronic patient record. This includes logging any additions or changes or deletions that are made to it. The scanned document and its linked clinical entry must be monitored by the audit trail and any changes made after initial scanning logged. The audit trail should also log who views a record or scanned document and when they viewed it. The ability to log a record view is desirable, but not mandatory, in the Requirements for Certification 2007. This will become manadatory in the next round of certification testing.

8. Shredding

To shred or not to shred, that is the question. In an ideal world a practice would scan all documents into the electronic patient record and archive the originals. The reality of storage and archive costs means that this is not possible. Section 22 of the Electronic Commerce Act 2000 deals with the admissibility of evidence and states:

> *In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility in evidence of—*
>
> *(a) an electronic communication, an electronic form of a document, an electronic contract, or writing in electronic form—*
>
> *(i) on the sole ground that it is an electronic communication, an electronic form of a document, an electronic contract, or writing in electronic form, or*
>
> *(ii) if it is the best evidence that the person or public body adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form,*

Thus it would be reasonable for practices to shred scanned documents providing:

- Staff are properly trained in the use of the practice management system;
- The process of scanning documents follows the recommended guidelines;
- The audit trail of the practice management system is robust;
- Safe data backup procedures are in place;
- Provision is made for future proofing, i.e. the ability to access and interpret the documents in the future;

The destruction of original documents must be done in a way that ensures that they are completely and confidentially destroyed. Thus documents to be shredded must be clearly identified in the practice and a cross-cut shredder used to ensure the strips can not be reassembled. Some practices allow a delay between scanning and shredding: scan one day, check back up went ok the next day and then shred.

If third party contractors are used to destroy records by shredding, pulping or incineration then the service contract must ensure confidentiality and certificates of destruction must be obtained.

9. Backup

Three things in a practice are irreplaceable: the staff, the patients and the data. If your practice was to have a catastrophic fire or flood and these three elements were saved, then you could be up and running in 24 hours with all the information you need to continue to provide care. One of the commonest causes of data loss is failure of a hard disk drive.

9.1 Hard Disk Crash

The biggest study of hard drive failure was published by Google in February of 2007 (http://labs.google.com/papers/disk_failures.pdf). As you might imagine, Google uses a lot of hard drives, more than one hundred thousand of them. The research shows that 1.7% of disk drives failed in their first year of operation, 8% percent failed during their second year and 8.6% in their third year. If your hard drive shows a scan error then it is 39 times more likely to fail within 60 days than drives without scan errors.

9.2 Backup Plan

Retrieving data from crashed disks is expensive and often incomplete. It is critical to ensure your practice has a well defined working backup system. Focus on the risks and the consequences and then develop a plan. This should include:

- Daily backup of data;
- Taking a backup off site daily;
- Having a backup routine that allows you to go back a day, a week or a month, in case your data gets corrupted;
- Assigning one person in the practice with responsibility for backup;
- Contracting with a company to provide you with a backup system, teach your staff how to monitor it and verify that it works;

In terms of off site backups, practices are advised to make a formal contractual arrangement with a company to store backups in a safe environment.

Advice on information security and backup can be found in the document "No Data No Business" available from the GPIT Group at http://www.icgp.ie/gpit.

10. References

Good practice guidelines for general practice electronic records (version 3.1). Department of Health & Royal College of General Practitioners. June 2005. Available from http://www.dh.gov.uk/assetRoot/04/11/67/07/04116707.pdf

Protecting Personal Health Information in Ireland: Law and Practice. Peter Lennon. Cork: Oak Tree Press; 2005.

Risk Manager for GP. Kieran Doran, Ann O'Driscoll, Catherine Murray, Paula Hodson, Asim Sheikh, Siobhan Prout. Dublin: Thomson Round Hall; 2002.

Electronic Commerce Act 2000. Available from http://www.irishstatutebook.ie/2000_27.html

No Data No Business: General Practice ICT Security Guidelines and Checklist, available from http://www.icgp.ie/gpit

General Practice Software Management Systems: Requirements for Certification 2007, available from http://www.icgp.ie/gpit