



Standards for patient confidentiality and PACS



RCR Standards

The Royal College of Radiologists (RCR), a registered charity, exists to advance the science and practice of radiology and oncology.

It undertakes to produce standards documents to provide guidance to radiologists and others involved in the delivery of radiological services with the aim of defining good practice, advancing the practice of radiology and improving the service for the benefit of patients.

The standards documents cover a wide range of topics. All have undergone an extensive consultation process to ensure a broad consensus, underpinned by published evidence where applicable. Each is subject to review four years after publication or earlier if appropriate.

The standards are not regulations governing practice but attempt to define the aspects of radiological services and care which promote the provision of a high-quality service to patients.

Current standards documents

Standards for providing a 24-hour interventional radiology service

Standards for the communication of critical, urgent and unexpected significant radiological findings

Standards for Self-assessment of Performance

Standards for Radiology Discrepancy Meetings

Standards in Vascular Radiology

Standards for Ultrasound Equipment

Standards for Iodinated Intravascular Contrast Agent Administration To Adult Patients

Standards for Patient Consent Particular to Radiology

Standards for the Reporting and Interpretation of Imaging Investigations

Cancer Multidisciplinary Team Meetings – Standards for Clinical Radiologists

Technical Standards for Ultrasound Equipment

360° Appraisal – Good Practice for Radiologists

Individual Responsibilities – A Guide to Medical Practice for Radiologists

Contents

Foreword	4
1. Introduction	5
2. Background	6
2.1 <i>Duty of confidentiality</i>	6
2.2 <i>Guidance from the Department of Health</i>	6
3. The Data Protection Act (1998) and Caldicott Principles	7
3.1 <i>The Data Protection Act (1998)</i>	7
3.2 <i>The Caldicott Principles</i>	7
4. The use and misuse of PACS	8
4.1 <i>The use of PACS</i>	8
4.2 <i>The misuse of PACS</i>	8
5. Patient information and compact discs	9
6. Standards for patient confidentiality and PACS	10
6.1 <i>Standard 1</i>	10
6.2 <i>Standard 2</i>	10
6.3 <i>Standard 3</i>	10
6.4 <i>Standard 4</i>	10
6.5 <i>Standard 5</i>	10
6.6 <i>Standard 6</i>	10
6.7 <i>Standard 7</i>	10
References	11
Audit	11

Foreword

With a move towards an increasingly IT-based medical world, the issue of patient confidentiality comes to the fore. Patients expect that information about them will be held in confidence by their doctors and doctors have a duty to maintain this confidentiality.

While many patients understand and accept that information must be shared within the healthcare team in order to provide their care, it is essential that medical information is handled carefully and remains fully protected.

The advent of picture archiving and communication systems (PACS) in radiology brings its own challenges as regards security but confidentiality in PACS must be maintained on the same basis as any other aspect of the practice of medicine.

This document aims to set standards for how patient confidentiality should be maintained with specific regard to the use of PACS. These standards should complement, but not replace, the legal, professional and contractual obligations that already are in existence.

The College is grateful to the Standards Sub-Committee comprising Dr Richard Fitzgerald, Dr Richard Nakielny, Dr Alan Freeman, Dr Fergus Gleeson, Dr Huw Lewis-Jones, Dr Robert Manns, Dr Sue Barter, and Officers of the Faculty of Clinical Radiology, for their help in producing this document; with particular thanks to Dr Jane Adam (Chair) and Dr Jonathan Ellis (who led on this standard).

Comments on drafts of the standard from members of the Clinical Radiology Patients' Liaison Group, members of the Standards S-C e-Consultation panel, and elected members of the Clinical Radiology Faculty Board were also very much appreciated.

Dr Tony Nicholson

Vice-President and Dean
Faculty of Clinical Radiology
The Royal College of Radiologists

1. Introduction

Confidentiality is a cornerstone of medical practice, and forms the foundation of the doctor–patient relationship. There are ethical, contractual and legal obligations to ensure that patient information is passed within a confidential framework, and to ensure information is held in a safe and secure manner.

The increasing availability of picture archiving and communication systems (PACS) both within hospitals and between hospitals means that a further category of patient information (contained in medical images and imaging reports) is available to those with access. Information contained within a PACS system is subject to the same confidentiality constraints as any other patient data held electronically, and doctors are obliged professionally to treat this information with the same ethical regard to confidentiality that would be afforded to a clinical consultation.

2. Background

2.1 *Duty of confidentiality*

A duty of confidentiality typically arises from three drivers: the practitioner's professional or regulatory body, the contract of employment, and the law.

For radiologists, the General Medical Council document *Good Medical Practice*¹ clearly states a doctor's duty of confidentiality, 'Patients have a right to expect that information about them will be held in confidence by their doctors. You must treat information about patients as confidential, including after a patient has died'.

Contracts of employment will typically contain confidentiality clauses and state that breaches of this confidentiality may lead to formal disciplinary action by the employer.

There is a body of legislation which makes misuse and unauthorised access to information held on a computer a criminal act. This legislation includes the Data Protection Act (1998).²

2.2 *Guidance from the Department of Health*

As well as common law and statute, the Government also issues guidance through the Department of Health on patient confidentiality. Of particular note are the *Confidentiality: NHS Code of Practice*³ (2003) and *The Caldicott Guardian Manual 2006*.⁴ This latter guidance is based upon the *Report on the Review of Patient-identifiable Information* in 1997 by the Caldicott Committee.⁵

To attempt to summarise all the above statute and guidance may be simplistic, but essentially information should only be passed on a *need-to-know basis*.

3. The Data Protection Act (1998) and Caldicott Principles

3.1 The Data Protection Act (1998)

The eight principles of the act are as follows.²

1. Personal data shall be processed fairly and lawfully, and in particular, shall not be processed unless at least one of the conditions in *Schedule 2* is met, and in the case of sensitive personal data, at least one condition in *Schedule 3* is also met.[†]
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in a manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensure an adequate level of protection of the rights and freedoms of data subject in relation to the processing of personal data.

Although all of the principles apply to patient confidentiality and PACS, Principle 2 (Personal data shall be obtained only for one or more specified and lawful purposes) and Principle 7 (Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing) are perhaps most relevant, while Principle 8 (Personal data shall not be transferred to a country or territory outside the European Economic Area) becomes relevant where PACS and teleradiology are employed together.

3.2 The Caldicott Principles

The Caldicott Report⁵ set out principles that healthcare organisations should use when processing patient information. A major recommendation of this report was that flows of patient identifiable information should be justified and tested against the principles defined in the report.⁵ The six principles are as follows.

1. Justify the purpose(s).
2. Do not use personally identifiable information unless it is absolutely necessary.
3. Use the minimum personally identifiable information.
4. Access to personally identifiable information should be on a strict need-to-know basis.
5. Everyone should be aware of their responsibilities.
6. Understand and comply with the law.

Although all the Caldicott Principles apply to patient confidentiality and PACS, Principle 4 (Access to personally identifiable information should be on a strict need to know basis) and Principle 5 (Everyone should be aware of their responsibilities) are perhaps most relevant.

[†] = The conditions of Schedule 2 and Schedule 3 are detailed in the Act,² and both state that patient consent is needed.

4. The use and misuse of PACS

PACS provides both a record of the medical image and the radiology report relating to that image. PACS brings both enormous potential to improve radiological care delivery but at the same time brings significant risk to patient confidentiality.

4.1 *The use of PACS*

The day-to-day use of PACS is likely to include all or some of the following:

- (i) Analysis and review by healthcare professionals involved in the care of the patient
- (ii) Review by a wider healthcare professional audience at a multidisciplinary team meeting
- (iii) Review by radiologists during a discrepancy meeting
- (iv) Teaching of healthcare professionals by radiologists or clinicians
- (v) Review of images and/or reports for the purposes of clinical audit
- (vi) Review of images and/or reports for the purposes of research.

Whereas many radiologists might instinctively feel that the use of PACS is justified in all of the above categories, the image was probably obtained from the patient on the implicit understanding that it would be used in their medical care. The patient might not be aware that their information might be used, for example, in teaching or audit. Data Protection Act Principle 2 (Personal data shall be obtained only for one or more specified and lawful purposes) and Caldicott Principle 4 (Access to personally identifiable information should be on a strict *need-to-know basis*) could be interpreted as being in conflict with the use of PACS in anything other than direct medical care.

Informed consent prior to obtaining a medical image might offer a solution, although this is unlikely to be practicable in many circumstances.

4.2 *The misuse of PACS*

The potential for improper use of PACS is considerable, and includes the following.

- (i) Casual browsing of images and reports by staff not involved in the care of the patient.
- (ii) Browsing of images and reports by individuals not authorised to access PACS following a lapse in access security.

Although one instinctively thinks of patients who might have a raised public profile or other healthcare staff, the issues apply equally to all patients.

Data Protection Act Principle 2 (Personal data shall be obtained only for one or more specified and lawful purposes) and Principle 7 (Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing) are most relevant in these scenarios of misuse as is Caldicott Principle 4 (Access to personally identifiable information should be on a strict *need-to-know basis*).

5. Patient information and compact discs

It is current practice to copy some patient images and reports on to compact discs (CDs). This method is typically employed when the care of a patient is being transferred from one centre to another, but may simply be needed to allow the patient to be discussed at a multidisciplinary team meeting at another hospital. This approach is needed where there is no link between the PACS systems of the different centres involved in the care of the patient.

It is also common practice to encrypt this information in an attempt to increase the security of the data. In some cases, however, the hospital receiving the CD does not have the necessary equipment to decode the encryption. This will delay discussion of the contents of the CD and can present a risk to the clinical care of the patient.

6. Standards for patient confidentiality and PACS

As there already exist clear professional, contractual and legal obligations of patient confidentiality, the College does not seek to re-state these duties in this document. Instead, the College recommends standards based on clarity within organisations about how these duties should be executed.

6.1 Standard 1

Radiologists should be aware of their professional, contractual and legal responsibilities with regard to viewing PACS data, and abide by these obligations.

6.2 Standard 2

Radiology departments should work with their Caldicott Guardian and IT department to establish, publish and enforce a clear local policy on access and use of PACS.

6.3 Standard 3

Radiology departments should facilitate induction teaching for new users clearly stating the duty of confidentiality.

6.4 Standard 4

The local development of electronic audit trails of PACS usage is encouraged to ensure that all image-viewing on PACS can be justified. Users should be reminded of ongoing audit of use every time they log on.

6.5 Standard 5

Radiology departments should work with their Caldicott Guardian to establish clear local guidance on the use of PACS for teaching, audit and research. This might take the form of a local agreement that if patient confidentiality is maintained then such usage is acceptable.

6.6 Standard 6

Where electronic links and/or teleradiology services are used by radiology departments, trusts should satisfy themselves that the patient information is handled, at every stage, with the same degree of protection that would apply to information processed within the trust. This is especially relevant if the data is transferred outside the European Union.

6.7 Standard 7

Where CD copies of patient images are produced, suitable security measures should be employed by trusts to ensure that the information remains protected. This includes provision of secure storage and means of physical transfer of discs.

Approved by the Board of the Faculty of Clinical Radiology: 20 June 2008

References

1. General Medical Council. *Good Medical Practice*. London: GMC, 2006.
2. Data Protection Act (1998). http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 (last accessed 25/09/08)
3. Department of Health. *Confidentiality: NHS Code of Practice*. London: DH, 2003. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253 (last accessed 25/09/08)
4. Department of Health. *The Caldicott Guardian Manual 2006*. London: DH, 2006. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_062722 (last accessed 25/09/08)
5. The Caldicott Committee. *Report on the Review of Patient-Identifiable Information*. London: DH, 1997.

Audit

An audit template is in preparation and will be available on AuditLive on www.rcr.ac.uk

Citation details:

The Royal College of Radiologists. *Standards for patient confidentiality and PACS*. London: The Royal College of Radiologists, 2008.

ISBN: 978-1-905034-34-5 Ref No. BFCR(08)15 © The Royal College of Radiologists, November 2008

For permission to reproduce any of the content contained herein, please email: permissions@rcr.ac.uk

This material has been produced by The Royal College of Radiologists (RCR) for use internally within the National Health Service in the United Kingdom. It is provided for use by appropriately qualified professionals, and the making of any decision regarding the applicability and suitability of the material in any particular circumstance is subject to the user's professional judgement.

While every reasonable care has been taken to ensure the accuracy of the material, RCR cannot accept any responsibility for any action taken, or not taken, on the basis of it. As publisher, RCR shall not be liable to any person for any loss or damage, which may arise from the use of any of the material. The RCR does not exclude or limit liability for death or personal injury to the extent only that the same arises as a result of the negligence of RCR, its employees, Officers, members and Fellows, or any other person contributing to the formulation of the material.

Design by innov8 graphic design: www.innov8gd.com. Printed by Gallpen Colour Print.