Standards for patient confidentiality and RIS and PACS
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 improving the service for the benefit of patients by defining best practice, and promoting advances in practice.

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.

All of the standards produced by The Royal College of Radiologists can be found on the College website www.rcr.ac.uk/standards

Current standards documents

- Standards for the communication of critical, urgent and unexpected significant radiological findings, Second edition
- Standards for patient consent particular to radiology, Second edition
- Standards of practice and guidance for trauma radiology in severely injured patients
- Standards and recommendations for the reporting and interpretation of imaging investigations by non-radiologist medically qualified practitioners and teleradiologists
- Standards for the NPSA and RCR safety checklist for radiological interventions
- Standards for the provision of teleradiology within the United Kingdom
- Standards for the recording of second opinions or reviews in radiology departments
- Standards for a results acknowledgement system
- Standards for intravascular contrast agent administration to adult patients, Second edition
- Standards for the introduction of new procedures and new devices - updated in January 2010 to reflect new guidance from the MHRA on ‘off label’ use
- Standards for radiofrequency ablation (RFA)
- Standards for providing a 24-hour diagnostic radiology service
- Standards for patient confidentiality and PACS
- Standards for providing a 24-hour interventional radiology service
- Standards for Self-assessment of Performance
- Standards for Radiology Discrepancy Meetings
- Standards for the Reporting and Interpretation of Imaging investigations
- Cancer Multidisciplinary Team Meetings – Standards for Clinical Radiologists
- Standards for Ultrasound Equipment
- Standards for patient confidentiality and RIS and PACS
Contents

Foreword 4
1. Introduction 5
2. Background 6
   2.1 Duty of confidentiality 6
   2.2 Guidance from the Department of Health 6
3. The Data Protection Act (1998) and Caldicott Principles 7
   3.1 The Data Protection Act (1998) 7
   3.2 The Caldicott Principles 7
4. The use and misuse of PACS 8
   4.1 The use of PACS 8
   4.2 The misuse of PACS 8
5. Patient information and compact discs 9
6. Standards for patient confidentiality and PACS 10
   6.1 Standard 1 10
   6.2 Standard 2 10
   6.3 Standard 3 10
   6.4 Standard 4 10
   6.5 Standard 5 10
   6.6 Standard 6 10
   6.7 Standard 7 10
References 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 those caring for them and doctors and other clinicians 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) and associated radiology information systems (RIS) brings its own challenges with regard to 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 and RIS. These standards should complement, but not replace, the legal, professional and contractual obligations that already are in existence.

The Royal College of Radiologists (RCR) is grateful to Dr Tony Newman Sanders for reviewing and updating this publication. The previous document, BFCR(08)15 Standards for patient confidentiality and PACS, has now been withdrawn.

Comments on drafts of the standard from members of the Clinical Radiology Patients’ Liaison Group, members of the Professional Support and Standards Board, elected members of the Clinical Radiology Faculty Board and members of the Imaging Informatics Special Interest Group were also very much appreciated.

Dr Pete Cavanagh

Dean, Clinical Radiology – Vice-President, 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 professional, ethical, contractual and legal obligations to ensure that information entrusted to healthcare professionals remains within a confidential framework, and to ensure that this information is held in a safe and secure manner.

The increasing use of electronic information systems in healthcare provides a new set of challenges to the maintenance of patient confidentiality. Picture archiving and communication systems (PACS) have now been deployed across the NHS throughout the UK and their use both within and between hospitals and other healthcare organisations means that, with their associated radiology information systems (RIS), they contain far more patient information than any other UK healthcare information system. Several million patient studies are archived in local and regional data stores and tens of thousands of studies are electronically shared each year between organisations adding immeasurably to the quality and safety of patient care. This has required radiologists and other healthcare professionals to rethink and redefine what this means for their relationship with patients and their duty to safeguard confidentiality.
2. Background

2.1 Duty of confidentiality

The common law duty of confidentiality is central to the professional standards implicit in practising as a healthcare professional and is articulated and upheld by the various professional and regulatory bodies. Numerous elements of statute law pertain to this duty which is usually also reflected in contracts of employment with healthcare organisations.

For radiologists, the General Medical Council document *Good Medical Practice* 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’.


Key patient identifiable information includes:

- Patient’s name, address, full post code, date of birth
- Pictures, photographs, videos, audio-tapes or other images of patients
- NHS number and local patient identifiable codes
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

2.2 Guidance from the General Medical Council

In addition to the summary guidance contained in *Good Medical Practice*, the GMC has issued detailed guidance on confidentiality in 2009. Separate guidance on making and using audiovisual recordings is also available.

2.3 Guidance from the Department of Health and the NHS

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* (2003). The DH issued supplementary Guidance to the code in 2010 on the disclosure of patient information in the public interest. Other relevant DH Guidance includes *NHS Code of Practice on Information Security Management* (2007), *NHS Information Governance: Guidance on Legal and Professional Obligations* (2007). The *NHS Constitution* (2012) restated that patients have a right to privacy and confidentiality and to expect the NHS to keep confidential information safe and secure. The NHS Care Record Guarantee was updated in January 2011.

2.4 Caldicott Principles

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.

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 in PACS, Principle 2 and Principle 7 are perhaps most relevant, while Principle 8 becomes relevant where PACS and teleradiology are used to outsource reporting to other jurisdictions.

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

3.2 The Caldicott Principles

The Caldicott Report13 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. 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 and Principle 5 are perhaps most relevant.
4. The use and misuse of PACS and RIS

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. RIS usually provides the platform for workflow within imaging departments from booking patients to reporting. It is the usual interface with other electronic patient systems including results requesting (Ordercomms) and results notification and other interfaces with the wider electronic health record (EHR).

4.1 The use of PACS

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

- Analysis and review of images and/or reports by healthcare professionals involved in the care of the patient
- Review by a wider healthcare professional audience at a multidisciplinary team meeting
- Review by radiologists during a discrepancy meeting
- Teaching of healthcare professionals by radiologists or other clinicians
- Review of images and/or reports for the purposes of clinical audit
- Review of images and/or reports for the purposes of research
- All the above uses may be deployed across organisations using wide area image and report sharing. They may also be used across jurisdictions using teleradiology. Even if it can be assumed that all those who will have access to these data are effectively involved in the care of the patient, imaging departments need to assure themselves that any third parties are subject to the same, or better, information security and governance as the host organisation, such that implicit consent can continue to be inferred and that patients should not be concerned about loss of control of their data. If data are to be transferred outside the European Union, explicit consent must be obtained.

It is acceptable to assume the implicit informed consent of patients that images and reports containing their patient identifiable data (PID) will be shared with other members of the healthcare team responsible for their care for the purposes of delivering appropriate clinical care and for local clinical audit purposes. Consent can be implied if patients have been given enough information to understand that they can, if they wish, opt out of sharing their PID. Due care needs to be given to ensuring that such information is made available in such a way that all patients are likely to be able to understand how their data are likely to be used in the normal course of providing clinical care. This could include material in appointment letters, posters in waiting rooms, information leaflets and appropriate entries on organisational websites. Imaging departments need to be able to respect patients’ wishes if they decide that they do not want PID to be shared. Often this may mean respectfully informing the patient that their care cannot be provided.

In general, it will be possible and desirable to anonymise PACS images and reports and associated clinical data for these purposes. Special care needs to be given to obtaining implicit or explicit consent from children. As stated above, if image data are transferred outside the European Union the patient’s explicit consent needs to be obtained.

4.2 The misuse of PACS

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

- Casual browsing of images and reports by staff not involved in the care of the patient
- 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 removable media

It is still widespread practice to copy patient images and reports on to compact discs (CDs) and other removable media. 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. Following the loss of large amounts of patient data by HM Customs and Excise, clear direction was given to NHS organisations mandating the use of secure encryption of all such media including memory sticks, laptops and CDs. Clarification of this guidance to allow for some local discretion, subject to rigorous case by case risk assessment, was published by Connecting for Health (CfH) to avoid situations where critical clinical information could be delayed by an inability to decrypt in an emergency situation. The increasing widespread use of the Image Exchange Portal (IEP), Accenture PACS Connect, BT PACS Exchange and other accredited means of electronically transferring images and reports has greatly reduced the requirement for using portable media. It is hoped that the use and functionality of these services is maintained and continues to increase. Electronic transfer is currently the mechanism of choice for transferring these data.
6. Standards for patient confidentiality and PACS

As there already exist clear professional, contractual and legal obligations of patient confidentiality, the RCR does not seek to re-state these duties in this document. Instead, the RCR 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. Staff working in imaging departments should all have a clear understanding of the duty of confidentiality and should be supported by written and other materials to ensure that all patients are in a position to give implied informed consent for the normal use and sharing of their imaging data to deliver their healthcare and support local clinical audit.

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. Imaging departments should provide assurance that regular audits of usage do occur and that inappropriate use is investigated and, if necessary, disciplinary procedures invoked. The use of ancillary systems such as IEP should also be subject to regular audits.

6.5 Standard 5
Radiology departments should work with their Caldicott Guardian to establish clear local guidance on the use of PACS for teaching, research and other secondary uses, including policies and protocols for obtaining explicit consent if such data cannot be anonymised. Local policies should be agreed with the involvement of local patient representative groups, and written information about the agreement, and opting out of data sharing, should be made available to patients. Robust procedures should be in place for ensuring the anonymisation of data used for such purposes, including training in the use of anonymising functions of PACS. Further work is needed to promote and standardise the use of the Digital Imaging and Communications in Medicine (DICOM) anonymiser products.

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 are transferred outside the European Union. With the advent of widely available electronic sharing of data, radiologists and their organisations should remember that the risk of breaching patient confidentiality is greatly increased and makes it even more important to adhere to Caldicott principles. There should be a transparent and effective way of obtaining explicit consent for transfer of data outside the EU.

6.7 Standard 7
Where patient image data are stored or transferred using portable electronic media, suitable security measures should be employed by trusts to ensure that the information remains protected. This includes provision of encryption, secure storage and safe modes of transporting such media. Radiologists should be familiar with their own organisations’ policies on confidentiality and data security.

Approved by the Board of the Faculty of Clinical Radiology: 15 June 2012
References
