www.rcr.ac.uk

Clinical Radiology
The Royal College of Radiologists

Guidance on maintaining patient confidentiality when using radiology department information systems

Second edition

November 2019

Contents

Introduction

Radiology information systems (RIS), picture archiving and communication systems (PACS), Order Comms and electronic patient record (EPR) systems facilitate the rapid and widespread distribution of sensitive patient data and images within and beyond the institution where they were initially acquired. This may be for diagnosis, second opinions, multidisciplinary team meetings (MDTMs), audit or research. Thousands of images and often their reports are transferred daily around the NHS, to research centres and also to the independent sector via the image exchange portal and other bespoke connections. However, patients rightfully expect only those with a legitimate reason to do so access their data. As such, radiologists must be mindful of the duties of confidentiality placed on them by law, in particular the Data Protection Act (DPA) 2018 and the European Union's General Data Protection Regulation (GDPR) 2016.[1,2] Radiologists are also bound by the professional obligations of the General Medical Council (GMC) as well as local information governance and contractual requirements. This is no different to the way other doctors are required to maintain patient confidentiality on ward rounds, in clinics, in general practice (GP) surgeries and so on.

This document provides information on what to do in commonly encountered data-sharing situations. With this knowledge, and the application of common sense, radiologists should be in a better position to comply with the law and provide the level of confidentiality that patients expect. A note of caution however; data confidentiality and the legislature surrounding it are complex and constantly evolving. You are strongly advised to seek the guidance of your local data protection officer (DPO) before commencing any new patient data handling processes.

Note 1: For the purposes of this document the terms images, reports, patient information and patient data are used synonymously.

Note 2: This document does not include guidance for PACS office staff or information technology (IT) managers nor does it describe how to store electronic data in a secure manner. This information should be sought from local IT departments, information governance officers (IGO) and DPOs.

Acknowledgements: Members of the RCR Radiology Informatics Committee (RIC); Mr Mark Scallan, Head of Information Governance, Royal Cornwall Hospital.

1. Definitions

Personal data is defined by GDPR and the DPA as any information relating to an identifiable natural person.[1,2] The data subject is generally someone who can be identified, directly or indirectly, by reference to a name or NHS/hospital number. However, physical, physiological, genetic, cultural and social identities are now also included in this definition.

Data concerning health is termed special (category) data and is subject to a higher standard of protection.

Data processing is the recording or holding of any personal data, its retrieval, consultation, alignment, combination, adaptation, alteration, erasure, destruction, transmission to third parties or disclosure. GDPR says that processing of health data is prohibited unless:

- The patient has given explicit consent
- It is necessary for medical diagnosis, treatment, occupational or preventative health
- It is in the interests of public health (that is, ensuring high-quality healthcare and the safety of devices and medicines)
- Complying with a legal obligation to which the Data Controller (see below) is subject.

In short, healthcare organisations will have to be more careful with their data, more exact in knowing where it is stored, how it is processed and whether consent for processing has been given.

Data controllers – organisations such as hospitals are required by law to appoint a data controller who determines the purposes for which data processing is performed. Stand-alone clinics, consultants and those undertaking medico-legal work are also likely to be viewed as data controllers for any patient information they process and are subject to the same enforcement, prosecution and compensation provisions under the DPA if they breach the law.

Note 1: Failure to register data processing activities with the Information Commissioner's Office (ICO) is a criminal offence and carries a £5,000 fine.

Note 2: Any breaches in data security must be notified to the ICO within 72 hours.

Note 3: The ICO has the power to impose a penalty of up to £500,000 where a breach of the DPA causes 'substantial damage or distress'.

Note 4: Breaches of the GDPR are subject to fines of twenty million Euros or 4% of annual turnover, whichever is the greater.

Data processor is someone who processes personal data on behalf of the data controller.

Data protection officer (DPO) – GDPR requires all public authorities to have a DPO. Their role is to inform and advise their organisation(s) about all issues in relation to GDPR compliance. Smaller organisations that do not process information on a large scale are not legally required to appoint a DPO but are still subject to GDPR if they handle special (such as health-related) data. The processing of patient data by individual physicians does not constitute large scale processing but if you are part of a group that provides radiology services to the independent sector, for example, you may consider it prudent to appoint a DPO. More information is available on the ICO website.[3]

National Data Opt Out (NDO) – this is a new service that allows people to prevent their confidential data being used for research or planning. It was introduced on 25 May 2018. It does not apply to anonymised data. Guidelines on expectations for anonymisation (and how

it differs from pseudonymised data) are due to be published by the Information Governance Alliance in due course.[4]

Note: the NDO automatically replaces NHS Digital's former 'Type 2' opt-out.

Vital interests – you may access or disclose information in life or death situations, for example when treating an unconscious trauma patient admitted through the emergency department. However, you may not do so if the patient is able to give consent but refuses (assuming they are competent to do so). You should be prepared to justify your reasoning.

Vital interest is less likely to apply when care is planned in advance.

Subject access requests (SARs) – under GDPR, data subjects are entitled to gain access to their personal data free of charge and within one month of receipt of their request. (This can be extended to sixty days where the request is excessive or unreasonable.)

2. Basic guidance on confidentiality

Radiology departments should protect patient information by:

- Recognising that confidentiality is an obligation for all staff, external contractors, volunteers and students. Radiology departments must ensure all relevant individuals are appropriately trained so that confidentiality is maintained.
- Recording patient information accurately and consistently while avoiding jargon, abbreviations, speculation and personal opinion.
- Not discussing patient information inappropriately or where there is a risk of being overheard.
- Keeping information secure.
  - Laptops, tablets and mobile phones holding patient information should not be left unattended in cars or other accessible areas.
  - Computers must be password protected and logged out when not in use. Patient information must not be visible to other patients or passers-by.
  - Passwords should never be shared and should be changed regularly. It is an offence under the Computer Misuse Act 1990 to gain unauthorised access to computer material, including using another person's ID without authority.
  - Except for the purposes of audit, research or teaching it is not appropriate to 'browse' PACS, RIS or other electronic systems or interrogate them for patient information with which you have no legitimate relationship.
  - Patient information should not normally be removed from the workplace unless specific local rules have been agreed.
  - Offices should be kept locked and cupboards secured.
- Disclosing information with appropriate care.
  - Follow established rules for sharing information with external organisations (see *Section 4. Transfer of patient data to remote organisations and devices*).
  - Check that persons requesting information are genuine and have a legitimate reason to access that information.
  - Share only the minimum information required.
  - If in doubt, do not share information.

Be mindful of the Caldicott Principles (of 1997)

1. Justify the purpose(s) for using confidential information.
2. Don't use confidential information unless it is absolutely necessary.
3. Use the minimum amount necessary.
4. Access should be on a strict need-to-know basis.
5. Be aware of your responsibilities.
6. Comply with the law.

The Information Commissioner has acknowledged a nervousness among healthcare professionals about breaking confidentiality and the potential fines therein. The Information Governance Review of 2013 found these concerns could be significant barriers to improvements in patient care and experience. As such a seventh Caldicott Principle was added:

7. The duty to share information can be as important as the duty to protect patient confidentiality.

Furthermore, when appointed National Data Guardian for Health and Care in 2014, Dame Fiona Caldicott committed to three additional principles:[5]

Principle 1 – to encourage the sharing of information in the interests of providing direct care to an individual.

This was countered by **Principle 2** – there should be 'no surprises' to citizens and they should have choice about the use of their data.

Principle 3 encourages dialogue with the public to increase their knowledge and choices about how their data are used to improve healthcare.

Patients must be informed effectively – 'no surprises'.

- Patients must be aware that their information is being recorded, may be shared with other healthcare professionals involved in their direct care, used in clinical audit and monitored to assess the quality of care. If you consider they might not be aware then they are not being correctly informed.
- When dealing with particularly sensitive information you should be explicit about what is being recorded and ensure the patient is happy with this.
- Patient information leaflets and notices must be easily readable and accessible.
- It is good practice to tell patients if you intend to share their information with anyone else. For example, 'I am going to send this information to your GP/to the consultant looking after you.' It is also important to inform patients their information may be shared with other organisations that may become involved with their care such as independent choose and book or private providers. Regional and national specialist centres and second opinions also fall into this category.
- When information is likely to be used for purposes other than direct care and clinical audit, you should expect to gain explicit consent, that is, the patient has agreed via a positive act for their information to be shared, in words or orally (see *Section 3. Consent to share data*).

Restriction of disclosure

- Respect patients' decisions to restrict the disclosure of their information. It may not be possible to do this without compromising their care but ultimately it is their decision. You should record this decision and demonstrate that their right to future safety and healthcare provision will not be affected and that they are free to change their minds at a later date.

Breaches

- You should report any breaches of confidentiality to your line manager, IGO or DPO at the earliest opportunity.

3. Consent to share data

Traditionally, consent to share patient data has been viewed as either implied or explicit with:

- **Implied consent** – being sufficient when sharing data in the context of direct care or clinical audit
- **Explicit consent** – required for everything else.

However, **GDPR** has introduced two important new concepts.

- Organisations (such as hospitals) that process personal data must establish and publish the lawful basis on which they do so.
- Relying on consent alone is only valid in limited circumstances. Furthermore Article 4 (11) requires that this consent be given by a statement or clear affirmative action and must be freely given, specific, informed and unambiguous.[2]

This sets a high bar and means that existing consent-based models for sharing data may no longer be legal. Information on how to obtain consent and lawfully process data should be obtained from the IGOs and DPOs at your host institution but in the meantime you may choose to observe the following.

- GDPR section 9 (2) (h) says that lawful processing by all publicly funded healthcare organisations is permissible in the delivery of direct care and its administrative purposes for, '... medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems ...'[2]
- Section 6 (1) (e) allows processing during direct care for '...the performance of a task in the public interest...' (such as ensuring high-quality healthcare and the safety of devices and medicines).
- The ICO says you should only access patient information:
    1. To support a patient's direct care or if you are satisfied that the person you are sharing the information with is accessing or receiving it for that purpose
    2. If you are satisfied that anyone you disclose personal information to understands you are giving it to them in confidence, which they must respect
    3. If you are satisfied that patients have been informed how their information will be used, they have had the right to object and have not objected. (Information can be provided in leaflets, posters and on websites. It should be tailored to their communication requirements as far as practicable.)
    4. For the purposes of clinical audit.

- For all instances where you are involved in the acquisition or interrogation of patient data for purposes other than direct care (or clinical audit) you should expect to obtain explicit consent or have reason to believe that it has been obtained.
- The Information Governance Alliance has published guidance on GDPR, the DPA and consent, available via the NHS Digital website.[6] It has also consulted on the limitations of implied consent and will publish its recommendations soon.[7]
- Remember, if a patient withdraws their consent you will have no legal basis to process personal data about them.

4. Guidance on specific instances of data sharing and confidentiality

Sharing data during radiological practice

GDPR allows you to process personal patient data for the purposes of:

- Medical diagnosis, treatment and its associated administration, for the purposes of direct care
- Managing healthcare systems, for example during service improvement exercises (see *Section 3. Consent to share data*).

Explicit, affirmative consent must be obtained when sharing information for all other purposes (unless the information is fully anonymised).

GDPR also says, 'any new processing of health data requires a Data Protection Impact Assessment (DPIA) and you must inform your local Data Protection Officer (DPO) where relevant'.[2]

Clinical audit

The General Medical Council (GMC) says, 'all doctors in clinical practice have a duty to participate in clinical audit. You may disclose personal information to your team or those working to support them on the basis of implied consent, as long as you are satisfied that it is not practicable to use anonymised information and that the patient:

- Has ready access to information that explains that their personal information may be disclosed for local clinical audit (such as information sheets)
- Has the right to object and have not objected'.

Radiology events and learning (REAL) meetings

This activity highlights repeated omissions and misinterpretations and thus enhances patient safety. It is a type of clinical outcome review programme and is categorised as a form of clinical audit by the GMC. As such, information may be disclosed on the same basis.

Research

Patient data collection (including imaging) and sharing within the NHS and UK academic institutions must be done within an appropriate information governance framework.

- Any data relating to a living person, where identification is reasonably likely, is classified as sensitive (special category) data. Sharing this data requires explicit consent.
- If this has not been obtained the GMC and GDPR say that you may only disclose anonymised or coded recordings for use in research.[2,8]

- Notes on levels of anonymisation:
  - You should be aware that even trivial details may allow for re-identification and you should be particularly careful when using information from modalities that 'burn' patient identification data (PID) into images such as ultrasound, nuclear medicine, computed tomography (CT) and image intensifier dosimetry summaries. Also, beware when sharing volume data sets of the potential for facial reconstruction.
  - Be aware that 'pseudonymised' data (where codes or other identifiers are split from the rest of the patient data set but kept within the same organisation) may still be classified as sensitive (special category) data depending on how difficult it is to re-attribute that identifier whether through legitimate, reckless or deliberate intent.
  - 'Anonymise' functions on some modalities and PACS systems may strip most identifiers but leave behind dates of birth and details of referring clinicians. Motivated intruders, a term used by the ICO, could use this information to re-attribute images to patients.
  - Specifically:
    - Names and hospital numbers are direct and indirect identifiers respectively. Images with this information cannot be shared without explicit consent other than in the context of direct care.
    - Study ID numbers and hospital names can be shared with another NHS institution or UK universities but only if they are under the same contractual arrangements and have the same data stewardship arrangements. Commercial companies and charitable research organisations are not included in this provision and will require explicit patient consent.
    - Images that contain no name, date of birth, hospital or study ID number and no hospital name are deemed unidentifiable and can be used freely in the appropriate format. Consent is not required.
  - You should ensure that you record only the minimum data required for research purposes (data minimisation), that patients are able to consent only to areas of research relevant to them (granular consent) and that you are transparent when telling them how their information will be used and about their ability to opt out at any point.
  - As an individual radiologist you must ensure that material you use for research has been authorised by an appropriate institutional governance review board. Any research trial should be registered with the organisation's DPO and Caldicott Guardian.
  - Further information has been published by The Royal College of Radiologists (RCR) and also by the NHS Health Research Authority.[9,10]

Teaching, training and publications

- In general patients understand that the training and education of medical and allied healthcare professionals requires access to their details, including special category (healthcare) data. In most cases this training will be integrated into their role as part of delivering direct care; as such it would be expected and lawful for such trainees to have access to patient records just as any other clinician would, unless the patient objects to this access.

- If the training or education is part of a clinical encounter, such as an ultrasound list or reporting session for example, it is reasonable to classify this activity as part of the provision of care.
- The information about how patients' data is used should be clearly displayed within the organisations 'fair processing notices', both physical and electronic.
- If the trainee is not part of a team involved in the direct provision of care or connected in any way to a patient's treatment, anonymised/de-identified information should be used for education and training purposes. (Certain PACS platforms facilitate image display without identifiable information as an option. You should use this function wherever possible.)
- Any disclosure to clinicians not employed or acting in an official capacity of the organisation must be anonymised.
- If patients' explicit consent has not been obtained you should only keep identifiable information in a training record if you are satisfied it will be kept securely and will be managed in accordance with the guidance outlined in this document and the information governance requirements of your host institution.
- You should be very wary of holding any identifiable information in an external record. If you do this, you are likely to be viewed as a data controller and will need to register this with the ICO. As a minimum seek the advice of your local DPO before you do so.
- When teaching is delivered in a more generic context, fully anonymised information must be used. Advice on how to establish or submit cases to regional and national teaching archives is available through the RCR.[11]
- Never use presentation software (PowerPoint and so on) to crop PID from an image. A third party could then un-crop the image and gain access to the information.
- Any images used in publications must be fully anonymised.

Multidisciplinary team meetings (MDTMs), departmental meetings and seminars

- Identifiable information should only be used when all those present have a legitimate right to be there and are involved in the direct care of patients.
- Particular care should be taken when distributing images and other information over teleradiology links (virtual meetings). Again, you should ensure that participants at remote sites have a legitimate reason for being there.

Patients who lack capacity

- You should only disclose information about patients without capacity if the recipient is directly involved in the patient's care.
- In training situations this should only be done if there is no reasonable alternative, you cannot wait until the patient regains capacity or if you are permitted to do by a person with authority to make decisions on the patient's behalf.

Email

Ten rules to follow when sharing patient information:

1. Types of email accounts
   - Ideally you should only send patient information to accounts ending '@nhs.net'.
   - If you have to use another type of NHS account for example '@somewhere.nhs.uk', be sure of the identity of the recipient before you send it.
2. Do not import NHS mail account settings into your mobile device email client. (This means confidential information can potentially be stored on your device and then inadvertently backed up to the cloud). Only access email remotely using the NHS web portal.
3. Never auto-forward mail to other accounts.
4. Mark all email subject lines, 'confidential'. Do not include any patient information (including hospital or NHS numbers) in this line.
5. In the text, use the minimum number of patient identifiers, for example, NHS number only. Avoid using names and dates of birth where possible.
6. Delete emails that contain patient information as soon as practicable.
7. Think carefully about who you give proxy access to (for example, secretaries and personal assistants). Is it appropriate for them to see patient information?
8. Be very careful when using group email accounts, for example, for GP enquiries. These should only be set up after agreement with your IGO/DPO.
9. Be careful when replying to emails from patients or other members of the public. You have no way of knowing who may read it or where it may end up. It is good practice just to acknowledge receipt of such emails and to request verification of their legitimacy via other means such as standard mail or a telephone call. Limit the exchange of sensitive data as far as possible.
10. Remember, email has the same legal status as a letter, can be submitted as evidence in court and can also be requested via the Freedom of Information Act.

Transfer and sharing of patient data with remote organisations and devices

Other NHS providers

This would normally be via the image exchange portal (or IEP, shortly to be IEP 2.0 or equivalent) although numerous legacy peer-to-peer links exist. As a minimum, communication should be via encrypted NHS networks. In England this is the Health and Social Care Network (HSCN – which replaced N3 in 2017); in Wales, the Public Sector Broadband Aggregation (PSBA); and in Scotland, the Scottish Wide Area Network (SWAN). Within NHS regional clinical networks (for example, cancer and stroke) patients may have images archived on multiple PACS systems. Most radiologists can only view images held in their local PACS archives (unless already transferred via IEP). With future technological advances it will be possible to access patients' images across sharing networks directly via local PACS viewers. (Some networks are already doing this, for example, Scotland, Merseyside and the East Midlands Radiology Consortium [EMRAD].) This 'patient-centric' approach to sharing patient data across multiple regional PACS enhances care. It must be

noted though that the local PACS should always keep an audit log of all access to patient data, whether held locally or remotely.

To independent sector (IS) providers

Patient data transfer may be to an IS NHS (choose and book) or non-NHS provider. Where possible, communication should also be via the IEP. If no link has been established, peer-to-peer virtual private networks (VPNs) may already exist or encrypted CDs may be used. As for NHS providers, patient confidentiality must be maintained by:

- Ensuring patient data transmission only occurs to *bona fide* locations and that the staff therein are fully aware of their confidentiality obligations under the DPA and GDPR
- CDs are only given to staff members with a legitimate reason to receive them. A record must be kept of the patient concerned, CD number, its contents and the name and designation of the staff recipient.

CDs for patients

These should only be handled by the local medical records department or equivalent body.

Out-of-hours image review and reporting provision

Increasing numbers of radiologists are reporting images remote from their host institutions, whether as individuals or as part of reporting networks. Various architectures exist, with and without shared RIS and PACS instances. Minimum requirements for ensuring patient confidentiality include:

- All data transmissions should occur over HSCN or regional equivalent
- If using a device issued by the host IT department check it has suitable authentication routines applied. Access via a VPN, username and password authentication is usually sufficient
- If using a personal device, triple authentication may be required, for example username, password and security token
- Images, reports and other patient data should clear from any system cache at the end of every network interaction session
- Only radiologists with a direct involvement in patient care should access patient data
- All radiologists with access to a reporting network should be recorded by the network owner prior to network go-live
- A DPIA should be performed prior to any network go live.

Transfer of personal data outside the EU

GDPR places specific exclusions on the transfer of patient data beyond member states of the EU and EEA; examples might include remote computational analysis of cardiac CT data. With the exception of specific organisations listed on the EU-US Privacy Shield website you should only send personal data outside the EU with the affirmed consent of the patient and inform your local DPO before doing so.[12]

Social media and instant messaging apps

Little or no case law exists surrounding the transfer of patient information via these applications. Sending reminders for appointments via SMS (text) message is acceptable if it contains appointment information only. Information sent via other applications such as WhatsApp are encrypted end-to-end but there can be no guarantee that the intended recipient is the only individual with access to the remote device. You should take advice from your local IGO and DPO before sharing any sensitive personal data with patients or colleagues using such platforms. Further guidance is available from NHS Digital, but in brief:[13]

- Ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device's address book
- If you are an instant messaging group administrator, take great care when selecting the membership of the group and review the membership regularly
- Switch on additional security settings such as two-step verification
- Review any links to other apps that may be included with the instant messaging software and consider whether they are best switched off
- Separate your social groups on instant messaging from any groups that share clinical or operational information
- Unlink the app from your photo library.

Fax

There have been multiple data breaches through the inadvertent transmission of patient information to incorrect fax numbers. Although primary care providers frequently fax patient request cards and letters to imaging departments (at their own risk), radiologists and departments should only use fax to communicate patient information in emergencies and when more secure methods are unavailable.

Note 1: eFax is a more secure alternative to conventional fax and its use should be considered.

Note 2: All fax machines must be phased out of the NHS by 31 March 2020.

Removable media (CDs, DVDs, USB sticks and flash drives, smart phones, tablets, digital cameras and so on)

- Removable media should only be used to store or transfer information as a last resort. Under normal circumstances information should be stored and transmitted on the established healthcare systems described above and exchanged using appropriately protected and approved information exchange portals.
- All removable media should be provided by and registered to your organisation. They must be password protected and hold the information in an encrypted format.
- Any transmission of patient data using screen shots on non-secure devices is inherently dangerous and should not happen.

Recordings made by patients

- With respect to exemptions from the GDPR and DPA (2018) the ICO says: 'personal data processed in the course of a purely personal activity, with no connection to a professional or commercial activity, is outside the GDPR's scope. This means that if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the GDPR'.
- Guidance from the MDU states the following:[14]
  - You may not like a patient recording you but your duty of care means you would not be justified in refusing to continue to treat them. If you did, it could rebound on you and further damage your relationship with the patient. Remember that your refusal to continue with the consultation could also be recorded.
  - If a friend or relative of the patient performs the recording you should ensure the patient is happy for this to continue.
  - You may ask for a copy of the recording for your own records but the patient is under no obligation to provide you with one.
  - Audio and video recordings have been used in court as evidence but so long as you are performing a competent examination and behaving in an appropriate manner you should have nothing to worry about. Indeed the recording may help support your case.
- The GMC also says, 'You must give patients the information they want or need to know in a way they can understand. You should make sure that arrangements are made, wherever possible, to meet patients' language and communication needs.'[15]
- Patients and their relatives should be made aware that exemptions to the GDPR and DPA (section 'a', above) only apply in the context of purely personal processing. Other staff members with whom they have no relationship may have just cause for complaint if they consider they have been included unnecessarily in any footage.

Artificial intelligence and computer assisted diagnosis

The relationship between AI and data protection legislation is evolving. One incident in 2017 resulted in rebuke from the ICO following the transfer of 1.6 million patient records from a hospital to an AI company. The ICO published four 'lessons learned'.[16]

- It's not a choice between privacy and innovation – shortcomings in data handling were avoidable.
- Don't dive in too quickly – privacy impact assessments must be carried out before not after data transfer.
- New cloud processing technologies mean you can, not that you should – always apply a proportionality principle before transferring patient data.
- Know the law and follow it – don't ignore the Data Protection Act.

It also challenged the hospital's belief that testing an AI application prior to use in the clinical setting qualified as direct care.

Patients and their data must be protected. The sharing of fully anonymised patient information with AI and other IT companies should not breach the DPA although particular care will need to be taken with studies where identifiable information is burnt into the image (ultrasound for example).

The RCR's position statement on AI can be viewed online.[17]

In summary, GDPR and the DPA 2018 have significantly enhanced protections around patient identifiable information. You should only assume you have a lawful basis to share patient data when you are providing direct healthcare or are performing clinical audit. You should exercise care and judgement in all other situations, including research and teaching, when de-identification of data should be considered.

5. Further notes on disclosure

General

Disclosure is any passing of information to a person other than the patient.

You should be very cautious when asked to disclose information to third parties, even the police. There are certain situations when this is permissible or even required by law, however, you should always:

- Weigh up the benefits of disclosure against the rights of the patient to confidentiality and divulge only the bare minimum information required
- Consult your IGO or legal affairs officer before complying with requests. Your medical defence organisation may also be able to offer advice outside office hours
- Inform the patient what you are disclosing and why (unless doing so defeats the purpose of the disclosure)
- Document your reasons for doing so.

Reasons to disclose information include:

- **Coroners' investigations** – the coroner is required to investigate the circumstances of certain deaths. You are obliged to disclose any information you may hold about the deceased that is likely to be directly relevant to the investigation.
- **Civil and criminal courts** – a judge or presiding officer can require you to disclose patient information in various circumstances. You should highlight the lack of patient consent and should object to the judge or the presiding officer if attempts are made to compel you to disclose what appear to you to be irrelevant information, for example, matters relating to relatives or partners of the patient who are not party to the proceedings. The patient whose information is sought should be told about the order, unless that is not practicable or would undermine the purpose for which disclosure is sought.
- **The Driver and Vehicle and Licensing Agency (DVLA)** – the DVLA is legally responsible for deciding fitness to drive and needs to know if a driver has a condition or treatment that may affect their safety as a driver. The driver is legally responsible for informing the DVLA if they are unsafe but if they refuse to do so you should speak to them and contact the DVLA if they continue to drive against your advice. You should write to the patient informing them of your action.
- To other bodies:
  - **NHS Counter Fraud Investigations** – under the NHS Act 2006
  - **The GMC** –investigation of a doctor's fitness to practise under the Medical Act 1983

  - **The CQC, Health and Public Service Ombudsmen** – under acts of Parliament such as the Health and Social Care Acts.
- **Communicable diseases, knife or gunshot injuries** (although it would normally be the team with clinical responsibility for the patient to take these decisions).

Children

- A child can give consent aged 13 or over (a change in the DPA 2018, reduced from 16 years previously).
- The same duties of confidentiality apply when using, sharing or disclosing information about children and young people as adults. You should only share information if:
  - You are required to do so by law or in response to a court order
  - Abuse or neglect is suspected. (It would be unusual for a radiologist to do this without involvement of the local paediatric team.)
  - The young adult gives explicit consent or consent has been obtained from someone authorised to act on the child's behalf
  - It is justified in the public interest.
- If it is necessary to share information you should:
  - Disclose information that identifies the child only if necessary to achieve the purpose of the disclosure – in all other cases you should anonymise the information before disclosing it
  - Inform them about the possible uses of their information
  - Keep disclosures to the minimum necessary
  - Be mindful that older children can be very sensitive about keeping information confidential from parents, school and the police. However, it is vital that doctors have the confidence to act on their concerns about the possible abuse or neglect of a child or young adult.

Further guidance on disclosure is available from the GMC.

This document was approved by the Clinical Radiology Professional Support and Standards Board on 10 May 2019.

References

1. UK Government. *Data Protection Act 2018.* Norwich: The Stationery Office, 2018.
2. https://gdpr-info.eu/ (last accessed 4/10/19)
3. https://ico.org.uk/for-organisations/guide-to-data-protection/ (last accessed 4/10/19)
4. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-sharing-resources (last accessed 4/10/19)
5. National Data Guardian. *National Data Guardian for health and care 2017 report: Impact and influence for patients and service users.* London: National Data Guardian, 2017.
6. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-sharing-resources#information-sharing-responsibilities (last accessed 4/10/19)
7. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance (last accessed 4/10/19)
8. www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/using-and-disclosing-patient-information-for-secondary-purposes (last accessed 4/10/19)
9. The Royal College of Radiologists. *Guidance on the use of patient images obtained as part of standard care for teaching, training and research.* London: The Royal College of Radiologists, 2017.
10. www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/ (last accessed 4/10/19)
11. The Royal College of Radiologists. *Setting up a regional or national radiology digital teaching archive.* London: The Royal College of Radiologists, 2018.
12. www.privacyshield.gov/welcome (last accessed 4/10/19)
13. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-governance-and-technology-resources (last accessed 4/10/19)
14. www.themdu.com/guidance-and-advice/journals/good-practice-june-2014/patients-recording-consultations (last accessed 4/10/19)
15. https://ico.org.uk/about-the-ico/news-and-events/blog-four-lessons-nhs-trusts-can-learn-from-the-royal-free-case/ (last accessed 4/10/19)
16. www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/good-medical-practice/domain-3---communication-partnership-and-teamwork (last accessed 4/10/19)
17. www.rcr.ac.uk/posts/rcr-position-statement-artificial-intelligence (last accessed 4/10/19)

Appendix 1. Notes on legislation

Common law

In general common law allows disclosure of confidential information if:

- The patient consents
- It is required by law, or in response to a court order
- It is justified in the public interest.

Even if these criteria are met the disclosure must still satisfy the requirements of the DPA.

The Data Protection Act (DPA) 2018

The DPA states that personal data must be:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

The Freedom of Information Act 2000 (England, Northern Ireland and Wales) and Freedom of Information (Scotland) Act 2002

These give the public access to information held by public bodies such as the NHS but does not allow patients access to their health records. This requires a subject access request via the DPA which covers data processed by any organisation and should be referred to the local medical records department.

The Human Rights Act 1998

This provides other safeguards regarding privacy protection. This is not inviolable when matters of national security and public safety are at stake. However any interference with this right must be necessary and proportionate in the knowledge that:

- There may be damage to the individual whose privacy will be breached
- Society has an interest in the provision of a confidential health service, and be balanced against...
- ... the public interest that will be achieved through breaching an individual's privacy.

GDPR 2016

- In 2016 The European Parliament and Council issued The General Data Protection Regulation (GDPR). It came into law on the 25 of May 2018 and both strengthens and unifies data protection for all individuals within the EU.
- It applies to both data controllers and processors and stipulates heavy fines for non-compliance (4% of organisation annual turnover or 20 million euros, whichever is the greater).
- It covers the personal data of any EU subject, regardless of the controller or processor's location.

- All requests for consent to use personal data will have to be easily understandable, accessible and using the minimum of legalese and jargon. The purpose of data processing must be clearly attached to the consent. It must be as easy to withdraw consent as it is to give it.
- Data breaches which may pose a risk to individuals must be notified to the Data Protection Authority within 72 hours and to affected individuals without undue delay.
- Organisations that engage in large scale processing of sensitive personal data must appoint a Data Protection Officer.
- Article 5 of the Regulation requires that data be:
  - Processed lawfully, fairly and in a transparent manner in relation to individuals
  - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
  - All reasonable steps must be taken to ensure that personal data is up to date and accurate. If not it must be erased or rectified without delay
  - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
  - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Appendix 2. Glossary

CQC – Care Quality Commission

DPA – Data Protection Act (2018)

DPIA – Data protection impact assessment

DPO – Data protection officer

EEA – European Economic Area

EPR – Electronic patient record

GDPR – General Data Protection Regulation (2016)

GMC – General Medical Council

HRA – (NHS) Health Research Authority

ICO – Information Commissioner's Office

IGA – Information Governance Alliance

LED – Law Enforcement Directive

MDT – Multidisciplinary team

MRC – Medical Research Council

SAR – Subject access request

Appendix 3. Further information

Department of Health. *Confidentiality: NHS Code of Practice*. London: Department of Health, 2003.

Access to UK legislation and Acts of Parliament at www.legislation.gov.uk/ukpga (last accessed 17/9/19)

GDPR at www.eugdpr.org/ (last accessed 17/9/19)

GMC guidance on confidentiality at www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp (last accessed 17/9/19)

NHS Health Research Authority (HRA) www.hra.nhs.uk/ (last accessed 17/9/19)

ICO https://ico.org.uk/ (last accessed 17/9/19)

ICO Scotland Office https://ico.org.uk/about-the-ico/who-we-are/scotland-office/ (last accessed 17/9/19)

Medical Research Council (MRC) www.mrc.ac.uk/ (last accessed 17/9/19)

NHS Digital https://digital.nhs.uk/home (last accessed 17/9/19)

Appendix 4. Audit of adherence to patient confidentiality requirements in radiological practice

Background

Keeping patients' personal information confidential is a key requirement of the 2018 Data Protection Act (DPA) and European Union's GDPR. Auditing how your personal practice and that of your workplace complies with the regulations is just as important as auditing your clinical work. The items listed below are possible topics for such an audit and will give you an idea of how compliant you are with the current regulations.

The cycle

Standards

Your place of work should:

1. Have a data protection officer
2. Have a policy on patient confidentiality reflecting the DPA (2018) and GDPR regulations
3. Have readily accessible information leaflets and signs advising patients on how you intend to process their data
4. Obtain explicit consent when patient data is likely to be processed for purposes other than direct care or clinical audit
5. Keep a record of all meetings that involve the display of patient identifiable information (PID)
6. Use anonymised images when teaching (except when teaching those staff directly involved in patient care)
7. Have a log that records all the PID-containing removable media it releases (for example CDs). Records should include the name and designation of the recipient
8. Make sure that staff members are aware of and adhere to the email 'ten rules to follow when sharing patient information'
9. Log all devices used to create radiology reports remote from the host environment
10. Perform a documented data impact assessment prior to sharing PID with any external organisation.

Suggested number of standards to audit – choose any six but always include 2 and 3.

Target

100% compliance

Assess local practice

1. Engage with departmental clinical governance officer/lead
2. Ask to see departmental data protection policy(s)
3. Ask to see patient information leaflets and assess their accessibility
4. Ask to see removable media logs
5. Ask radiologists to describe how they use anonymised images when teaching or discussing images with individuals not involved in the direct care of patients
6. Ask to see data impact assessments for instances of image sharing with external organisations.

Suggestions for change if target not met

Discuss outcomes with local IGO, DPO and Caldicott guardians. Re-audit as appropriate.

Resources

1. The Royal College of Radiologists. *Guidance on maintaining patient confidentiality when using radiology department information systems*. London: The Royal College of Radiologist, 2019.
2. The Royal College of Radiologists. *Standards for patient consent particular to radiology, second edition*. London: The Royal College of Radiologist, 2012.
3. www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality (last accessed 17/9/19)
4. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-sharing-resources (last accessed 17/9/19)

The Royal College of Radiologists
63 Lincoln's Inn Fields
London WC2A 3JW

+44 (0)20 7405 1282
enquiries@rcr.ac.uk
www.rcr.ac.uk
@RCRadiologists

The Royal College of Radiologists. *Guidance on maintaining patient confidentiality when using radiology department information systems, second edition.* London: The Royal College of Radiologists, 2019.

Ref No. BFCR(19)10