Confidentiality Code of Conduct

Contents

1. Introduction

1.1. South East Coast Ambulance Service NHS Foundation Trust (the Trust) recognises that it has a duty to safeguard the confidentiality of all person-identifiable and other sensitive information where a duty of confidence applies.

1.2. The obligation to keep certain information confidential arises out of the Common Law Duty of Confidentiality; UK General Data Protection Regulation 2016, Data Protection Act 2018; professional codes of conduct; colleague employment contracts and, within the NHS, the Caldicott Principles.

1.3. In combination, these duties and obligations place all colleague members with access to confidential information under a duty to keep that information safe and secure. It is therefore of paramount importance to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability provide a robust governance framework to manage confidential information

1.4. The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

1.5. The Trust fully supports the principles of corporate and information governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and colleagues and commercially sensitive information.

1.6. The Trust also recognises the need in certain circumstances to share patient information with other partner agencies in a controlled manner, which is consistent with data protection legislation, and, in some circumstances, in the public interest.

1.7. The principle behind this Confidentiality Code of Conduct Policy is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls.

1.8. This policy has been written to meet both legal requirements and NHS guidance.

2. Aims and Objectives

2.1. This policy has been produced to protect colleagues and third-party contractors by ensuring they are aware of legal requirements and best practice, so that these are not inadvertently breached.

2.2. The aims are to ensure that those who have access to confidential Information. Are aware of the legal framework governing confidentiality, and data protection legislation.

2.3. Understand their personal responsibility to comply with legislation and the potential consequences of failing to do so.

2.4. Are aware of the measures in place to ensure that information is managed appropriately and stored securely.

2.5. Know the circumstances in which information may legitimately be disclosed and whom to contact for guidance.

3. Definitions

3.1. **Person - identifiable data (PID**) is any information that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g., photograph) may be sufficient to identify an individual.

3.2. **Confidential information** can take many forms including clinical and colleague's records, audits, occupational health records etc. It also includes any Trust confidential information, such as that which is, commercially sensitive; due for future publication; or information that may, if disclosed, place an individual at risk. Such information may be held on paper or electronically and includes information stored on portable devices such as USB memory keys, laptops, tablets/iPads, mobile phones, and digital cameras.

3.3. **Sensitive data**, as defined in the UK General Data Protection Regulation 2016 is information that relates to a living individual's:

- Race.
- Ethnic Origin.
- Political Beliefs.
- Religion.
- Trade Union Membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex Life; or
- Sexual Orientation.

3.4. Requirements stated in legislation (e.g., information regarding In-Vitro Fertilization, Sexually Transmitted Infections, HIV and Termination of Pregnancy).

4. Arrangements

4.1. Legal Framework. The UK General Data Protection Regulation 2016 (UK GDPR) and Data Protection Act 2018 (DPA) governs the way in which person identifiable information may be processed.

4.2. **Data protection principles are as follows:**

- Information is used fairly, lawfully and transparently.
- Used only for the 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 necessary.

4.3. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

4.4. The Act places responsibility for compliance with the principles at both an organisational and personal level and colleagues should be aware that knowingly or recklessly obtaining or disclosing personal data unlawfully is a criminal offence.

4.5. Article 8 of The Human Rights Act 1998 (HRA) states that everyone has the right to respect for your private life, your family life, your home and your correspondence. This means that personal information about you including your medical records should be kept securely and not shared without your permission, except in certain circumstances.

4.6. The Health and Social Care Act provides exemptions in certain circumstances where the sharing of information is related to the greater public health including instances where consent has not been provided.

4.7. The Computer Misuse Act 1990 (CMA) makes it an offence to attempt to access or alter information when you are not authorised to do so. Colleagues are given access rights to personal data when their role requires it. Any attempts to access personal data that is not necessary to fulfil your role is a breach of confidentiality and possibly an offence under the CMA.

4.8. A Common Law Duty of Confidentiality arises when a person discloses information to another (e.g., patient to clinician) and (employee to employee) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from case law; a requirement established within professional codes of conduct; and must be included in all NHS employment contracts with links to the disciplinary procedures.

4.9. The Caldicott Principles link closely to those within the DPA and should be applied by all colleagues when making decisions regarding the use of sharing of personal data.

4.10. **Justify the need;**

- Only use patient identifiable information when absolutely necessary.
- Use the minimum required for that purpose.
- Access should be on a 'need to know' basis.
- Everyone must understand their responsibilities to protect the information.
- Everyone must understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.
- Inform patients and service users about how their confidential information is used.

4.11. **Disciplinary Procedures**

4.11.1. All colleagues need to be aware that non-compliance with this Policy by any person working for the Trust may result in disciplinary action being taken in accordance with the Trust's disciplinary procedure and could lead to dismissal for gross misconduct. This includes all paid, voluntary colleagues, contractors, and consultants with appropriate provisions to be detailed in contracts as required.

4.11.2. If you have concerns about this issue, please discuss with your Line Manager. To obtain a copy of the disciplinary procedure please discuss with your Manager, the Human Resources department, or access it on the Trust intranet.

4.12. **Disclosure of Confidential Information**

4.12.1. Personally identifiable data is held under legal and ethical obligations of confidentiality. Although there are exceptions, patients have the right to choose whether to accept a form of care and the information disclosure needed to provide that care. They can also choose whether information that can identify them can be used for non - healthcare purposes.

4.12.2. Where the Trust holds employee identifiable data this must follow the same principles and disclosure must meet the legal and ethical principles of confidentiality.

4.12.3. Generally, patient information should not be used or disclosed in a manner that might reveal their identity without their consent or with the appropriate legal basis. Detailed guidance on these issues may be obtained from the Department of Health publication: "Confidentiality: NHS Code of Practice 2003" the Trust's Caldicott Guardian or the Information Governance Department.

4.12.4. A range of policies are available on the Trust's intranet under the 'Policies and Procedures' pages.

4.13. **Accessing Trust systems which hold personal data.**

4.13.1. Our patients and employees expect the right to confidentiality and the confidence that their personal data is safe, secure, used for the purposes intended and with a legal basis to do so.

4.13.2. We **ALL** have a personal and professional responsibility to maintain confidentiality. Therefore, any access to ***Trust information systems which hold/process personal data*** comes with a degree of personal and legal responsibility.

4.13.3. Under no circumstances must Trust employees access a personal record or any other information system holding personal data without a legal and contractual basis.

4.13.4. Access to all trust systems is auditable. Trust employees must not access a personal record or any other information system holding personal data without a legal and contractual basis.

4.13.5. Failure to comply with the above will result in a breach of confidentiality.

4.13.6. ALL requests/access to identifiable information must be justified and have a legal basis. Some may also need to be agreed by the Trust Caldicott Guardian, Head of Information Governance and/or Trust **SIRO.**

4.13.7. It is breach of confidentiality for Employees, Volunteers, Students, Contractors with access to Trust systems to look at any information relating to their own Family, Friends, or Acquaintances unless they are directly involved in the patient's clinical care. Identified breaches may result in disciplinary action.

4.13.8. If you have any concerns about the disclosure or sharing of patient/employee information, then this must be referred to your Line Manager. If they are not available, then advice must be sought from an individual with the same or similar organisation responsibilities.

4.13.9. Alternatively, the Trust Head of Information Governance / Head of Legal Services should be consulted for advice.

4.14. **Confidentiality and Systems Audit Procedure**

4.14.1. All organisations have a responsibility under data protection legislation, namely the UK General Data Protection Regulations (GDPR) and Data Protection Act 2018 to ensure that appropriate security measures and role-based access controls are in place to protect the personal data that they hold, process and share.

4.14.2. This requires the Trust to establish robust, documented, control mechanisms to manage and safeguard confidentiality, including mechanisms for highlighting problems such as incidents, complaints, and alerts. The effectiveness of these controls must also be evaluated.

4.14.3. A key component of these 'Security' measures is to ensure the 'confidentiality, integrity and availability' of all information systems and services. These measures ensure that personal data is securely retained, shared with a legal basis.

4.14.4. This procedure outlines how this will be achieved and must be read in conjunction with this policy. It applies to all sites and both electronic and manual based systems, used by colleagues, which are purchased, developed, and managed by/or on behalf of, the Trust to hold personal data or Trust sensitive information.

4.14.5. It details the auditing of systems access to ensure compliance is maintained and allow for escalation where this is appropriate. The Trust additionally utilises policies and procedures underpinned with the completion of mandatory annual training, and this audit procedure to ensure correct role-based access is achieved.

4.15. **Telephone Enquiries**

4.15.1. Generally, requests for person identifiable data must be made in writing. However, in exceptional circumstances, it may be appropriate to respond to a telephone request where you are able to:

- Independently verify identity of the caller.
- Check whether they are entitled to the information they request.
- Take a switchboard number, verify it independently and call back.
- All requests must be supported by a written request.

4.16. **Requests for information by the Police and Media**

- **Any Police enquires whether in verbal or written format must be directed as follows:**

  The Trust Legal Services Department,
  Trust HQ,
  Crawley.

4.16.1. Any Media enquiries must be referred to the Trust Communications Team. Trust HQ Crawley.

4.17. **Specialised external portals**

4.17.1. The Trust provides dedicated external portals for access to the patient record where an approved validation process has occurred. This includes the CAD hospital portal and the ePCR Case summary portal as well as dedicated Application Programming Interfaces (APIs). These approved portals are available following a set process and should only be used by approved persons.

4.17.2. Where a multi - factor identification process is employed such as the ePCR Case summary access card, and a request to confirm this detail has been received this can be validated over a telephony or email call provide no new information is shared and only information provided by the caller is validated. This should only be completed by appropriate mangers such as Emergency Operations Centre Manager's (EOCM) and Team leaders etc.

4.17.3. In all instances verifying the requestors' identity is required and this must be documented appropriately.

4.17.4. Where there is any instance where new information is needed to be provided this must be referred onto the relevant department such as patient experience, Legal or Human Resources.

4.18. **Disclosure of Information to Other Employees of the Trust**

4.18.1. Information on patients/employees may only be released on a need - to - know/legal basis. Firstly, the requestor's identity must be confirmed and the purpose for requesting the information/right to know provided. **ALL** requests for information must be reviewed and agreed with appropriate line management or alternatively through liaison with the Trust Head of Information Governance/Information Governance Manager.

4.19. **Minimising Risk**

4.19.1. Do not discuss patients/employees in public places or where you can be overheard. Do not undertake confidential conversations within an 'open office' environment.

4.19.2. Do not leave any clinical records or confidential information unattended in an open / unsecure area. Ensure that any computer screens, or other displays of information, cannot be viewed by the general public.

4.19.3. Ensure that desktops, laptop, or iPads are either shut down or locked at all times when they are left unattended.

4.19.4. When undertaking agile/remote working colleague members are responsible for ensuring that ALL SECAmb information/data (including personal data in relation to patients, colleagues and any corporate information) is protected from the risks

which are faced whilst working remotely. The Trust Virtual Private Network (VPN) is to be used to access any Trust based systems.

4.19.5. You must also ensure that your Trust issued device is regularly connected to the network to ensure that security and software updates are applied.

4.19.6. All correspondence containing person identifiable information must be addressed to a named recipient and marked 'Confidential'.

4.19.7. Any personal information/data must be addressed to a person, a post holder, a clinical colleague, or a legitimate safe haven. Not to a department, a unit, or an organisation. In cases where mail is for a team, it must be addressed to an agreed post holder or team leader / manager.

4.20. **Use of External and Internal Post**

4.20.1. Internal mail containing confidential data must only be sent in a securely sealed envelope and marked accordingly with a named recipient and annotated e.g., 'Confidential' or 'Addressee Only', as appropriate.

4.20.2. External mail must also observe these rules. Special care must be taken with personal information sent in quantity, such as patient clinical records, or collections of patient records on paper, electronic or other media. These must be sent by recorded delivery or by an approved courier, to ensure that there are only seen by the authorised recipient(s). In some circumstances, it is also advisable to obtain receipt as proof of delivery, e.g., patient records to a solicitor.

4.20.3. A return address must also be used to ensure that in the event of non - delivery the mail is returned and not opened.

4.21. **Faxing**

4.21.1. Faxing is not a safe method of transfer and must only be used when absolutely necessary and when there are no other means available.

4.21.2. To reduce the risk, remove patient identifiable data from any faxes unless it is absolutely necessary, and you are faxing to a known secure and private area **(safe haven).**

4.21.3. Faxes must always be addressed to named recipients and include a cover sheet marked '**Confidential'.**

4.21.4. Always check the number to avoid misdialling and ring the recipient to check that they have received the fax.

4.21.5. If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.

4.22. **Storage of Confidential Information**

4.22.1. Paper-based confidential information must always be locked away when unattended, particularly at nights and weekends or when the building/office is unoccupied for a long period of time.

4.22.2. Electronic information such as e-mails, Microsoft Office documents, etc. must not be saved onto the desktop or hard drive of your PC or laptop but to the Trust's network in a team / department specific folder with appropriate role-based access controls. This ensures the security of the information and enables recovery should the document become lost as the network is backed up daily.

4.22.3. Removable media, e.g., USB memory keys or external drives, CD/DVDs must not be used to transport sensitive or identifiable Information unless they are encrypted.

4.22.4. If you are required to travel to a location outside of the Trust and must transport person-identifiable or sensitive information, the data must be encrypted whilst in transit. Seek advice from the IT Department if you do not have an encrypted laptop or USB memory key.

4.22.5. For further information and guidance, please refer to the Trust's Removable Media Information Security Policy, which is located on the Trust Intranet site under Policies and Procedures.

4.23. **Disposal of Confidential Information**

4.23.1. When disposing of paper-based person-identifiable information or confidential information always use Trust issued 'Confidential Waste' containers/shredders. Keep the waste in a secure place until it is collected for secure disposal.

4.23.2. Computer printouts must either be shredded or disposed of as paper based confidential waste.

4.23.3. CD/DVDs containing confidential information must be either reformatted or destroyed. Computer files with confidential information no longer required must be deleted from both the PC and the Trust server if necessary. Please contact the Trust IT Department for guidance.

4.23.4. Computer hard disks must be destroyed / disposed of through the Trust IT Department or by an approved third-party contractor. This ensures that all information is deleted from the disk, as re-formatting makes it possible to gain access to the original information. In all instances certificates of destruction must be issued and retained.

4.24. **Confidentiality of Passwords**

4.24.1. Personal passwords issued to or created by employees are confidential and must not be shared or written down.

4.24.2. Passwords must comply with the approved password complexity rules as set down by the IT department and changed to a new password at the designated scheduled times.

4.24.3. You will be provided with more information about password control etc. When you receive your training and / or password. Information relating to this and Cyber Security is included within the Trusts mandatory IG training.

4.24.4. Any attempt to breach security must be immediately reported to the IT Department and may result in disciplinary action. It could also result in a criminal investigation under the Computer Misuse Act 1990 and / or the Data Protection Act 2018.

4.24.5. Security breaches may include but are not limited to attempt to bypass or defeat the security systems attempt to obtain or use passwords or privileges issued to other employees.

4.25. **Emailing Confidential Information**

4.25.1. Email sent within the Trust (i.e., the sender and recipient both have an email address ending '@secamb.nhs.uk') is encrypted and therefore secure. However, colleagues sending / receiving confidential information in this way should save the data to their personal area in the network and delete the email following transmission / receipt to minimise the risk of the information inadvertently being forwarded on in error.

4.25.2. Please seek advice from your manager if you have the need, or possible need, to e-mail person-identifiable information externally.

4.25.3. Patient identifiers must be removed wherever possible, and only the minimum necessary information sent.

4.25.4. Special care must be taken to ensure the information is only sent to those recipients who have a legitimate reason / need to know. Always double check you are sending the mail to the correct person.

4.25.5. External transfers of confidential information, where deemed to be necessary, must be sent with "Confidential" of "Addressee Only" anywhere in the subject line, this is standard terminology.

4.25.6. If this method of transfer is to be used it is recommended that a 'test email' takes place prior to sending confidential information to ensure the correct recipient is reached.

4.25.7. Email must not be used as a storage system and any confidential attachments that need to be retained should be securely saved to the Trust network in a restricted folder and removed from the email account.

4.25.8. Under no circumstances must any type of patient / employee identifiable information, sensitive or confidential information be transmitted unencrypted. Due to its insecure nature any information transmitted over the internet without encryption must be considered to be in the public domain.

4.25.9. For more detailed information, please refer to the Internet and Email Policy held within the Trust's intranet site.

4.26. **Working at Home / Agile Working**

4.26.1. Colleagues may access web mail from home PCs. If accessing Confidential information via, for example, an attachment to an e-mail on a home computer, or accessing such data from removable media such as an encrypted USB memory key you must ensure that you do not save the data to your own computer / laptop. This creates an information security risk and breaches confidentiality.

4.26.2. Colleagues must refer to the **Trust Office 365 Guidance** for further information.

4.26.3. Confidential paper records must not be taken home. In exceptional circumstances, where this is deemed essential, approval must be sought from your manager. A signed log of the documents taken must be maintained to indicate what has been taken and when it is returned to Trust premises. You will be individually responsible for ensuring its security.

4.26.4. Ensure that any documents / electronic devices are packaged appropriately and placed in the boot of the car or carried on your person while being transported from your workplace. You must not let anyone else have any access to records or electronic devices

4.27. **Loss or theft of Confidential Information or Storage Devices**

4.27.1. In the event that any hard copy confidential information or electronic information storage devices (e.g. CD / DVDs, laptops, mobile phones, iPads etc.) are lost, stolen or misplaced, these incidents must be reported immediately in accordance with the Trust's Incident Reporting Policy (DATIX) & Procedure.

4.27.2. Thefts or loss of IT devices, including mobile phones, laptops, and iPads, must also be reported to the IT Department and the Head of Information Governance / SIRO immediately.

5. Responsibilities

5.1. It is the role of the Trust Board to define the Trust's policy and strategy in respect of the codes of confidentiality, considering legal and NHS requirements. The Trust Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

5.2. The Chief Executive has overall responsibility as the Accountable Officer.

5.3. The Caldicott Guardian (Chief Medical Officer) provides a focal point for patient confidentiality & Information sharing issues and is supported by the Head of Information Governance and Trust SIRO in this respect.

5.4. The Senior Information Risk Owner fosters a culture for protecting and using data and is responsible for managing Trust information risks and incidents.

5.5. The Information Governance Working Group (IGWG) is responsible for promoting information governance within the Trust and monitoring compliance with related policies, procedures and data protection legislation.

5.6. Managers within the Trust are responsible for ensuring that this Confidentiality Code of Conduct Policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

5.7. All colleagues, (whether permanent, temporary, or contracted), and Contractors are responsible for ensuring that they are aware of their responsibilities and for ensuring that they comply with them on a day-to-day basis.

6. Competence

6.1. All colleagues receive training on data protection, Caldicott and Confidentiality at induction and annually through the key skills up-date programmes.

6.2. All managers within the Trust can advise on confidentiality issues on request or be in a position to obtain this information.

7. Monitoring

7.1. The IGWG reviews any reported incidents related to information governance at its meetings and identifies actions to be taken to mitigate the risk or reoccurrence.

8. Audit and Review

8.1. The IT Department will review event alerts related to unauthorised attempts to access confidential electronic data or systems where not covered under the Confidentiality and Systems Access Audit Procedure and will inform IGWG of any incidents of this nature and actions taken to address them.

8.2. This policy will be reviewed every two years or sooner if new legislation is introduced, or if changes are needed to reflect the Trusts development of policies and procedures and the changing needs of the Trusts.

9. Equality Impact Appraisal

9.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following Nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

9.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.

9.3. An Equality Impact Appraisal has been completed to assess whether this policy is likely to have an adverse impact upon disparate groups.

10. References

- Data Protection Act 2018
- UK General Data Protection Regulation
- Common Law Duty of Confidentiality
- Human Rights Act 1998
- Health and Social Care Act 2001
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988
- Human Fertilisation and Embryology Act 1990
- Confidentiality: NHS Code of Practice
- The Caldicott Guardian Manual 2010 (DH)
- NHSx Records Management Code of Practice 2021

Appendix A: Key Questions for Confidentiality Decisions

A number of example questions around confidentiality are as illustrated below. These examples demonstrate how the requirements of law, ethics and policy are adequately addressed when making decisions about the use or disclosure of confidential patient information.

This information below is not exhaustive and has been produced as 'general guidance' only.

If in doubt as to whether the sharing of information should take place, then please contact the Trust Head of Information Governance for advice and guidance.

Q1) If the purpose served by disclosing is NOT 'Direct' healthcare or another medical purpose, then what is the basis for disclosing?

A) ALL public sector bodies must act in accordance with their legal obligations, responsibilities and abide by Data Protection Legislation.

Whilst the sharing of information under direct care purposes is permitted, disclosures to agencies / organisations for other purposes may not be.

Guidance must always be sought from the Head of Information Governance or Head of Legal Services prior to the release of any information.

Q2) Is disclosure either a statutory requirement or required by order of a Court?

A) Any disclosure that has either a 'Statutory Requirement' or 'Court Order must be complied with. Please contact the Trust Head of Legal Services for advice and guidance.

Q3) Is the disclosure needed to support the provision of 'Direct' Healthcare or to assure the quality of that care?

A) Patients understand that some information must be shared to provide appropriate care and treatment. Clinical audit conducted locally within organisations is essential to ensure that the quality of patient care is sustained and improved. Therefore, the Trust must ensure that there is sufficient information available to inform patients/employees about how their information is processed, recorded, and shared.

This information is available in the form of a Privacy Notice/Employee Privacy Notice and Patient/Employee Information leaflets, which must be easily available/accessible for view within the Trusts website.

Patients/Employees **MUST** have a clear understanding of how/why their personal information is used and how any concerns, objections or requested opt outs of disclosures should be recorded.

Q4) If not for healthcare, then is the disclosure needed to support broader medical purposes?

A) The provision of preventative medicine, medical research, health service management/improvement and risk stratification are medical purposes as defined in law. However, the sharing of such information does not fall within 'Direct Care' but under 'Secondary Care' purposes. If a patient's personal information is to be used for 'Secondary Care' purposes, then explicit consent is the first requirement. Where this is not possible then a **Section 251** is required. However, a Section 251 is only used in instances where it is impracticable to gain consent and is therefore limited to several organisations.
The use of aggregated data (non-identifiable) is permitted. This **MUST NOT** contain any patient identifiable information, which could be linked to the patient.

Such identifiers typically include Name, DOB, NHS number, Gender, Address.

Q5) Is the use of identifiable and confidential patient information justified by the purpose?

A) Where the purpose is not to provide direct healthcare or to satisfy a legal obligation then disclosure and the legal basis for sharing must be determined. In such instances, advice must be sought from either the Trust Head of Information Governance or Head of Legal Services.

Q6) Have appropriate steps been taken to inform patients about proposed disclosures?

A) The Trust has a legal obligation to inform Patients / Employees about how their information is used, stored, shared and the purpose for sharing.

This explanation is provided using Privacy Notices including an Employee Privacy Notice and Patient/Employee Information Leaflets which clearly explain how information is recorded, accessed, stored and shared.

Q7) Is the explicit consent of a patient needed for a disclosure to be lawful?

A) **Unless disclosure of identifiable information is:**

- Required by law or the courts.
- For direct healthcare purposes.
- Can be justified as sufficiently in the Public interest to warrant a breach of confidence then explicit consent is required.