



Review Sheet

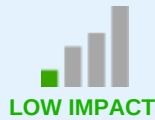
Last Reviewed
08 Sep '23



Last Amended
08 Sep '23

Next Planned Review in 12 months, or
sooner as required.

Business impact



Minimal action required circulate information amongst relevant parties.

Reason for this review

Scheduled review

Were changes made?

Yes

Summary:

This policy outlines the requirements for information governance, data protection and confidentiality. It has been reviewed with no significant changes. Further reading has been added and references have been checked and updated.

Relevant legislation:

- Care Quality Commission (Registration and Membership) (Amendment) Regulations 2012
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Medical Act 1983
- Mental Capacity Act 2005
- Mental Capacity Act Code of Practice
- Data Protection Act 2018
- The Health and Social Care Act 2008 (Regulated Activities) (Amendment) Regulations 2012
- UK GDPR



Underpinning knowledge - What have we used to ensure that the policy is current:	• Author: General Medical Council, (2022), <i>Confidentiality: good practice in handling patient information</i>. [Online] Available from: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality [Accessed: 8/9/2023] • Author: CQC, (2023), <i>Regulation 17: Good governance - Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17</i>. [Online] Available from: https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-17-good-governance [Accessed: 8/9/2023] • Author: Information Commissioner's Office, (2022), <i>Health and social care</i>. [Online] Available from: https://icosearch.ico.org.uk/s/search.html?collection=ico-meta&query=health+social+care&profile=default [Accessed: 8/9/2023] • Author: Department of health, (2013), <i>Information: To Share or not to Share - Government Response to the Caldicott Review</i>. [Online] Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF [Accessed: 8/9/2023] • Author: NHS, (2021), <i>Mental Capacity Act: making decisions for someone else</i>. [Online] Available from: https://www.nhs.uk/conditions/social-care-and-support-guide/making-decisions-for-someone-else/mental-capacity-act/ [Accessed: 8/9/2023] • Author: British Medical Association, (2021), <i>Confidentiality and health records toolkit</i>. [Online] Available from: https://www.bma.org.uk/advice-and-support/ethics/confidentiality-and-health-records/confidentiality-and-health-records-toolkit [Accessed: 8/9/2023] • Author: ICO, (2011), <i>The employment practices code</i>. [Online] Available from: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf [Accessed: 8/9/2023] • Author: NICE, (2018), <i>Decision-making and mental capacity - Guidelines NG108</i>. [Online] Available from: https://www.nice.org.uk/guidance/ng108 [Accessed: 8/9/2023] • Author: Primary Care Support England, (2023), <i>Accessing Medical Records</i>. [Online] Available from: https://pcse.england.nhs.uk/services/medical-records/accessing-medical-records-and-patient-details [Accessed: 8/9/2023] • Author: ICO, (2023), <i>Encryption scenarios - CCTV</i>. [Online] Available from: ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-scenarios/#12 [Accessed: 8/9/2023] • Author: NHS, (2023), <i>Records Management Code of Practice</i>. [Online] Available from: https://transform.england.nhs.uk/information-governance/guidance/records-management-code/ [Accessed: 8/9/2023] • Author: Department of Health and Social Care, (2003), <i>Confidentiality: NHS Code of Practice</i>. [Online] Available from: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice [Accessed: 8/9/2023]
Suggested action:	• Encourage sharing the policy through the use of the QCS App
Equality Impact Assessment:	QCS have undertaken an equality analysis during the review of this policy. This statement is a written record that demonstrates that we have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by equality law.



1. Purpose

1.1 Understand the key issues to take into account when making decisions on confidentiality in the face of increased access to electronic Patient information, the use of Patient information for secondary uses such as audit, commissioning, quality incentives and targets, research and teaching, and the confidentiality of personal identifiable information held on a valid basis about members of the staff and any others.

1.2 Identify important factors in making decisions around specific areas of Patient confidentiality and rights to confidentiality relating to children, adults who lack capacity and the deceased as well as the secondary uses of any personal identifiable information Lister House Surgery holds.

1.3 To ensure that Lister House Surgery demonstrates compliance with information governance responsibilities.

1.4 To support Lister House Surgery in meeting the following Key Lines of Enquiry/Quality Statements (New):

Key Question	Key Lines of Enquiry	Quality Statements (New)
EFFECTIVE	HE5: How are people supported to live healthier lives and, where the service is responsible, how does it improve the health of its population?	QSE4: Supporting people to live healthier lives
SAFE	HS3: Do staff have all the information they need to deliver safe care and treatment to people	QSS1: Learning culture QSS6: Safe and effective staffing QSS7: Infection prevention and control
WELL-LED	HW2: Is there a clear vision and credible strategy to deliver high-quality sustainable care to people, and robust plans to deliver?	QSW1: Shared direction and culture QSW5: Governance, management and sustainability

1.5 To meet the legal requirements of the regulated activities that {Lister House Surgery} is registered to provide:

- Care Quality Commission (Registration and Membership) (Amendment) Regulations 2012
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Medical Act 1983
- Mental Capacity Act 2005
- Mental Capacity Act Code of Practice
- Data Protection Act 2018
- The Health and Social Care Act 2008 (Regulated Activities) (Amendment) Regulations 2012
- UK GDPR



2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following Patients may be affected by this policy:

- Patients

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority



3. Objectives

3.1 To have the information and guidance (including competence, mental capacity, best interests and rights to confidentiality) required to identify and implement the definitive answers about disclosure of confidential information.

3.2 To make the right decisions about sharing information in response to third party requests and secondary uses that do not relate directly to a Patient's health or their active or ongoing healthcare and treatment.

3.3 This policy is part of the suite of data protection policies.



4. Policy

4.1 The Duty of Confidentiality - Patients, Staff and Associated Individuals

Lister House Surgery must ensure that Patients are fully involved in decisions about the use of their information. Patients must be assured that the information provided by them to Lister House Surgery is kept confidential and satisfied that any confidential information Lister House Surgery provides to others about them is with their consent, and relevant and up to date.

Confidentiality is an essential requirement for the preservation of trust between Patients and health professionals and is subject to legal and ethical safeguards. The knowledge that their information is treated as confidential is used to encourage people to seek appropriate treatment and share relevant information. Information about a Patient's health that they give in confidence will remain confidential unless there is a valid and compelling reason why it needs to be disclosed with or without their consent depending on both the circumstances and the law.

For the purposes of this policy, which goes into detail about Patient confidentiality, and in line with statutory requirements, the duty of confidentiality extends to all partners, members of staff of Lister House Surgery and all associated individuals who come into contact, or have the opportunity of coming into contact, with all or any personal identifiable information held by Lister House Surgery whether it relates to a Patient, a member of staff or an individual associated with Lister House Surgery.

4.2 Information to be Kept Confidential

All identifiable Patient information, including written, computerised, visual or audio records or information that exists in the memory of staff members at Lister House Surgery, is subject to the duty of confidentiality: This covers:

- Any clinical information about an individual's diagnosis or treatment
- A picture, photograph, video, audiotape or other images of the Patient
- Who the Patient's doctor is and what clinics Patients attend and when
- Anything else that may be used to identify Patients directly or indirectly so that any of the information above, combined with the Patient's name or address or full postcode or the Patient's date of birth, can identify them

Where the above identifiers are missing, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chance of Patient identification.

Whilst demographic information such as names and address are not legally confidential, they are often given by Patients in the expectation that this information will be kept confidential and the Patient's consent is sought prior to sharing it with third parties.

4.3 Using and Disclosing Information

In order to preserve confidentiality when a third-party requests information about Patients or their treatment, a number of factors must be considered including:

- Patients must be properly informed as to how identifiable information about them is used
- Data must be anonymised wherever possible
- Explicit consent must be sought for the use or disclosure of personal health information unless it is clearly implied
- When it is not practicable to obtain consent, information may be disclosed where the law requires or where there is an overriding public interest, e.g. where child abuse is suspected
- Disclosures must be kept to the minimum necessary to achieve the purpose
- When Patients withhold consent to disclosure of their information their wishes must be respected
- Health professionals and other staff members at Lister House Surgery must always be prepared to be accountable and justify their decisions about the use of personal health information

4.4 Consent

Consent to disclosure may be explicit or implied. It may also be consent to disclosure of specific information to a particular person or body for a particular purpose or it may be consent to general future disclosure for particular purposes. In either case consent must be informed and freely given.

Explicit or express consent is achieved when a Patient actively agrees, either verbally or in writing, to a particular use or disclosure of information. Explicit consent is the ideal as there is no doubt as to what has



been agreed.

Patient consent can be implied. In order for it to be valid Patients must be made aware that information about them will be shared, with whom it will be shared and of their right to refuse. Lister House Surgery is responsible for disclosures made which means being able to demonstrate that the assumption of consent was made in good faith and based on good information.

Information provided to Patients during a consultation, together with information enclosed with hospital/clinic appointment letters help to convey the reality and necessity of information sharing to Patients.

4.5 Anonymisation

Information may be used more freely if the subject of the information is not identifiable in any way, where clinical or administrative information is separated from details that might identify the Patient, e.g. name, date of birth and postcode.

Best practice recommends that Patients are informed of when and why their data is likely to be anonymised. Rare diseases, drug treatments or statistical analyses of small numbers within a small population may still identify some Patients so anonymisation must be undertaken individually according to the details about the Patient that are personally identifiable.

4.6 Pseudonymisation

Pseudonymisation is sometimes referred to as reversible anonymisation. Patient identifiers such as name, address or NHS number, are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.

Using the data with no means to reverse the process and identify any individual, it is treated as anonymised with no requirement to seek consent.

When someone has access to both pseudonymised data and the means to reverse the process, it must be treated as identifiable with Patients informed what information will be used and for what reason.

4.7 Sharing Information with Other Health Professionals

Patients are considered to have given implied consent for the use of their information by health professionals for the purpose of their health and the care they receive. Information sharing in this context is acceptable as health professionals share what is necessary and relevant for Patient care on a 'need to know' basis.

Disclosure of information to social services usually requires explicit consent from competent Patients, and an informed refusal to allow disclosure by a competent person must usually be respected. If the information is shared because the health professional believes it is a best interests decision then this must be recorded together with the justification.

4.8 Multi-agency Working

Integrated community teams are likely to comprise workers from health, social services and non-statutory bodies. To be able to use Patient data effectively within the team, Patient consent for sharing their information must be in place unless disclosure is required by law or there is an overriding public interest in disclosure.

4.9 All members of staff must be made aware of and be able to understand their responsibilities regarding confidentiality. Staff will enter into a written confidentiality agreement in a statement that forms part of their contract of employment to hold them contractually responsible for maintaining Patient, staff and other individual confidentiality at all times.

All members of staff who come into contact with personal health information in their work must be trained in confidentiality and security issues. Lister House Surgery must ensure that all staff members and others who work on site but are not necessarily employed by Lister House Surgery, e.g. cleaners, contractors and visiting health professionals, are aware of their ethical, legal and contractual duty of confidentiality and how to keep all confidential personal identifiable information secure from disclosure within the setting.

All contacts, discussions, conversations and instructions about clinical management of Patients, including phone calls from or about Patients will be confined to private spaces, e.g. offices, consulting, treatment and meeting rooms, in order to remain confidential and out of earshot of those staff and Patients not involved in the Patients' care as well as other members of the public.

4.10 Visitors and contractors who may get unplanned or accidental access to Patient or staff identifiable information will be asked to sign a confidentiality statement signifying their agreement to non-disclosure of any Patient or staff information to which they may gain access while on the premises going about their business, e.g. IT providers, building contractors etc.



5. Procedure

5.1 Operational Confidential Data Security - All records

For all types of records Lister House Surgery staff members will:

- Never inappropriately (without a valid reason) access records
- Shut and lock doors, offices and filing cabinets
- Wear ID if issued
- Query the status of visitors or strangers requesting or being given access on site
- Not tell unauthorised personnel how the security systems operate or provide them with login details for the clinical system
- Advise Lister House Surgery Caldicott Guardian or Andrew Smythe if anything suspicious or worrying is noted; and
- Confirm the identity of telephone callers and check the source of emails

Manual records

Manual/paper/hard copy records will be:

- Held in secure storage
- Booked out from their normal filing system and back in when they are returned
- Tracked if passed on to someone else in Lister House Surgery, with an update to record their current location within the file booking system
- Returned to the filing system as soon as possible after use with no unnecessary delay
- Stored closed when not in use so that the contents are not seen by others and locked away when Lister House Surgery is closed in accordance with the clear desk principles in the Security Policy and Procedure
- Inaccessible to members of the public; and
- Kept on site or at an agreed outsourced location, unless interim removal is essential, until they are recalled because the Patient has died or deregistered or it is no longer necessary to hold a member of staff's HR file after a relevant length of time according to the reason they are no longer employed

Electronic records

In the case of electronic records everyone must:

- Always log out of any computer system or application when work is finished
- Not leave a terminal unattended and logged in
- Not share Smartcards, login details or passwords with anyone else
- Change passwords at regular intervals, and on automatic system request, to prevent others who may have acquired them by any method unknown to the user from continuing to use them; and
- Always clear the screen of a previous Patient's information before opening and using another whilst consulting with patients

Emails

In the case of emails:

- Members of staff must be satisfied there are appropriate arrangements for the security of all personal identifiable information when it is stored, sent or received by computer, email or other electronic means
- Whenever possible, separate clinical details from demographic data
- All data transmitted by email must be encrypted, usually by using an NHS.net email account or other valid encryption method at the other end

Data retention and disposal

For GP Practices, all paper and electronic clinical records must remain with Lister House Surgery until a Patient registers at another surgery, dies or is otherwise removed/deregistered and their NHS general practice record is formally requested centrally for extraction.

Paper clinical records will be centrally requested for return via the NHS area paper records management



system.

The electronic record will be automatically or manually extracted when the Patient registers elsewhere or after they have been formally identified and notified as deceased.

In line with the Records Management Code of Practice and the ICO Employment Practices Code of Practice, Lister House Surgery will erase or anonymise personal data (e.g. staff, employment, administration and appropriate Patient non-clinical data) when it is no longer needed in order to reduce the risk of it becoming irrelevant, excessive, inaccurate or out of date.

Where there are deviations to the above due to local, contractual or insurance requirements, Lister House Surgery will ensure that the Patient, who is the data subject, is made aware of how their data will be processed and fair processing notices will be issued in line with GDPR and Data Protection Act 2018 requirements.

5.2 Recordings, Publication and the Media

Video and audio recordings and photographs

Recordings and photographs made for clinical purposes form part of the Patient's clinical record. These are subject to the same duty of confidentiality as all other personal identifiable information. The GMC advises that it is necessary to obtain the consent of the Patient, or, for a child, to obtain consent from someone with parental responsibility prior to a recording or photograph being made.

In relation to adults lacking capacity, video and audio recording must:

- Only take place if it is in the Patient's best interests
- Only be used for the purpose for which consent was granted
- Be stored securely; and
- Not be used for teaching purposes without consent if the Patient is identifiable

CCTV and surveillance

CCTV equipment will only be installed for a specific purpose, e.g. for the prevention and detection of crime, with staff and Patients made aware by notices where surveillance cameras are in use in public areas of Lister House Surgery. Lister House Surgery will follow the ICO guidance on the use of CCTV and the standards to be followed. Disclosure of CCTV footage (relevant images only) may be necessary, e.g. to the police with 'public interest' justification.

In line with the BMA and GMC stance on the use of covert surveillance, Lister House Surgery will 'obtain permission to make, and consent to use, any recording made for reasons other than the Patient's treatment or assessment'. In the exceptional circumstances where covert surveillance could be acceptable, e.g. strong evidence or suspicion of abuse, legal advice will be sought, and the involvement of police and social services agreed.

Call recording

No Patient calls will be secretly recorded, i.e. without the Patient's permission. Patient calls are confidential, and Patients will always be informed if their calls will be recorded when phoning Lister House Surgery. All recordings form part of the Patient's medical record and are accessible under the Data Protection Act.

Television, radio, internet and print

The BMA view is that publications, recordings, etc. are unlikely to be in the best interests of Patients. The Patient's written consent, for a child the written consent must be from someone with parental responsibility, is required for all publications or recordings for public access (including medical journals) whether or not the Patient will be identified. Patients must be informed that, by giving their consent to a publication or recording, they are unlikely to be able to withhold consent for its subsequent use. Permission must be obtained from everyone concerned and involved before Patients are filmed, recorded or quoted for wider or general public media consumption.

The press

While there is usually no reason to disclose confidential and identifiable information to the press, Lister House Surgery may be asked for information about individual Patients e.g.:

- To comment on the condition of a celebrity or otherwise well-known Patient. When the Patient has the capacity to make decisions about disclosure, consent is essential before any information is released to the media. When the Patient lacks capacity, legal advice must be sought
- After incidents involving harm to many people. During or after major disasters, e.g. a fire, road traffic accident, terrorist attack or outbreak of infectious disease, requests for information must be dealt with sensitively without breaching Patient confidentiality because it will not be necessary to include identifying or detailed clinical information about the people involved; or



- Where a Patient or a Patient's relatives use the press as a vehicle to complain about the treatment and care provided but Lister House Surgery is not permitted to 'set the record straight' and correct any inaccuracies, Lister House Surgery is limited to responding only by pointing out the information used is inaccurate or incomplete

5.3 Assessment of Capacity and Determining 'Best Interests'

The law presumes all people aged 16 and over have the capacity to give or withhold their consent to disclosure of confidential information about them, unless there is evidence to the contrary.

A Patient who is suffering from a mental disorder or impairment does not automatically lack the capacity to give or withhold their consent.

Patients who would usually be competent may be temporarily incapable of giving valid consent, and, therefore, incompetent and lacking capacity on purely a temporary basis, due to e.g. extreme fatigue, drunkenness, shock, fear, severe pain or sedation.

A Patient who has made a decision that appears to others to be irrational or unjustified cannot be conclusively regarded as lacking the mental capacity to make that decision. If the decision is clearly contrary to the Patient's previously expressed wishes, or based on a warped perception of reality, this may be a sign of a lack of capacity which will require further investigation.

Children and young people and capacity

People under 16 in England are presumed not to have capacity although, individually, they may be assessed as having the capacity to make their own informed decisions: they must demonstrate their competence by meeting legal standards, principally whether the young person has sufficient understanding and intelligence to understand fully what is proposed in order to consent based on the information they have received.

See Gillick competency and Fraser guidelines in Further Reading.

Factors to take into account when assessing capacity

To demonstrate capacity individuals will be able to:

- Understand in simple language (with the use of communication aids, if appropriate) what is to be disclosed and why it is being disclosed
- Understand the main benefits of disclosure
- Understand in broad terms the consequences of disclosure
- Retain the information long enough to use it in order to arrive at an informed decision
- Communicate the decision (by any means); and
- Make a choice that is free from pressure

Determining 'best interests'

All decisions taken on behalf of someone who lacks capacity must be taken in their best interests.

A best interests judgement is an objective test of what would be in the Patient's actual best interests taking into account all relevant factors, it is not about trying to make the decision the Patient is believed to have wanted.

A number of factors must be taken into account including:

- The Patient's own wishes (where these can be ascertained)
- The option that is the least restrictive for the Patient's future choices where there is more than one option from which to choose
- If the Patient is a child, the views of the parents; and/or
- The views of people close to the Patient, e.g. close relatives, partners, carers, welfare attorneys, court-appointed deputies or guardians, about what the Patient is likely to regard as beneficial

5.4 Adults Who Lack Capacity

Temporary or permanent mental incapacity

Most people suffering from a mental impairment can make valid decisions about some matters that affect them, and an individual's mental capacity must be judged in relation to the particular decision being made.

Therefore, where a Patient has the necessary level of capacity, disclosure of information to relatives or third parties requires the Patient's consent.

Relatives, carers and friends

Where a Patient lacks capacity, but has not given explicit consent for disclosure, information may need to be shared with relatives, friends or carers to enable healthcare professionals to assess the Patient's best interests but this does not mean all information will be routinely shared. Where the information is sensitive it



will be necessary to assess how much information the Patient is likely to want to be shared and with whom, and to respect evidence that the Patient did not want information shared.

Next of kin

'Next of kin' has no legal definition or status. If someone is nominated by a Patient as next of kin and given authority to discuss the Patient's condition, they may provide valuable information about the Patient's wishes although they cannot give or withhold consent to the sharing of information about the Patient and they have no rights of access to the Patient's medical records.

Next of kin must be nominated by the Patient and no-one can claim to be next of kin unless nominated by the Patient.

Proxy decision-makers

The Mental Capacity Act 2005 allows people over 18 years of age who have capacity to appoint a welfare attorney to make health and personal welfare decisions once capacity is lost. The Court of Protection may also appoint a deputy to make these decisions. Where a Patient lacks capacity and has no relatives or friends to be consulted, the Mental Capacity Act requires an Independent Mental Capacity Advocate (IMCA) to be appointed and consulted about all decisions about 'serious medical treatment', or place of residence. (An attorney or deputy can also be appointed to make decisions relating to the management of property and financial affairs).

In the case of health information, health professionals may only disclose information on the basis of the Patient's best interests, attorneys, deputies and IMCAs only need the information necessary to deal with the issue in question, not access to the whole of the Patient's records.

Where there is no attorney, deputy or IMCA, information must only be disclosed in the Patient's best interests.

Abuse and neglect

Where Lister House Surgery has concerns about a Patient lacking capacity who may be at risk of abuse or neglect, the concerns must be acted upon and information given promptly to an appropriate person or statutory body to prevent harm or further harm.

Where Lister House Surgery has doubts whether disclosure is in the Patient's best interests, Lister House Surgery will discuss the matter on an anonymous basis with a senior colleague, the Caldicott Guardian, their professional body or medical defence organisation. Lister House Surgery will ensure that their concerns and the actions taken, or they intend to take (including any discussion with the Patient, colleagues or professionals in other agencies) are clearly recorded in the Patient's clinical record by way of justification for the disclosure.

5.5 Legal and Statutory Disclosures

Disclosure required by statute

Health professionals are required by law to disclose certain information regardless of Patient consent. Health professionals must be aware of their obligations to disclose in these circumstances as well as to ensure that they do not disclose more information than is necessary.

Disclosure to the police, social services and partner organisations

Some statutes permit, rather than require, disclosure. In such cases, health professionals may only disclose information when the Patient has given consent or there is an overriding public interest.

Disclosure to solicitors

Health records that are required for legal proceedings are usually obtained via the Data Protection Act 2018 or Access to Health Records Act 1990. Health professionals releasing information to lawyers acting for their Patients must have the Patient's written consent to disclosure and, where there is any doubt, confirm that the Patient understands the nature and extent of the information disclosed.

Disclosure to courts, tribunals and regulatory bodies

The courts, including the coroner's courts, some tribunals and bodies appointed to hold inquiries, e.g. the General Medical Council, have legal powers to require disclosure, without the Patient's consent, of information that may be relevant to matters within their jurisdiction.

Statutory restrictions on disclosure

Health professionals are required by law to restrict the disclosure of some specific types of information, for example The Gender Recognition Act 2004 allows transsexual people who have taken decisive steps to live fully and permanently in their acquired gender to apply for legal recognition of that gender.

5.6 Public Interest

General principles

In the absence of Patient consent, a legal obligation or anonymisation, any decision whether identifiable information is to be shared with third parties must be made on a case by case basis and be justifiable in the



'public interest' i.e. the general welfare and rights of the public that are to be recognised, protected and advanced and essential to prevent a serious and imminent threat to public health, national security, the life of the individual or a third party or to prevent or detect serious crime. When considering disclosing information to protect the public interest, health professionals must:

- Consider how the benefits of making the disclosure balance against the harms associated with breaching the Patient's confidentiality both to the individual clinical relationship and to maintaining public trust in a confidential service
- Assess the urgency of the need for disclosure
- Persuade the Patient to disclose voluntarily
- Inform the Patient before making the disclosure and seek his or her consent, unless to do so would increase the risk of harm or inhibit effective investigation
- Disclose the information promptly to the appropriate body
- Reveal only the minimum information necessary to achieve the objective
- Seek assurance that the information will be used only for the purpose for which it is disclosed
- Document the steps taken to seek or obtain consent and the reasons for disclosing the information without consent
- Be able to justify the decision; and
- Document both the extent of and grounds for the disclosure

Research

The GMC advises doctors can now disclose identifiable information without consent for research purposes if it is in the public interest.

The BMA is of the view that, unless health professionals are confident they can make a reasonable assessment as to whether the research is in the public interest, a cautious approach should be adopted. In all cases, reasons for any disclosure must be documented.

Serious crime and national security

There is no legal definition as to what constitutes a 'serious crime' e.g. murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people. Serious harm to the security of the state or to public order and serious fraud will also fall into this category.

Theft, minor fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

Public safety

A common example of what can be categorised as public safety occurs in connection with the assessment of Patients with e.g. diabetes, epilepsy, defective eyesight, hypoglycaemia or serious cardiac conditions who have been advised by Lister House Surgery to discontinue driving but who continue regardless. Public safety may also be connected with risks arising from legitimately possessed firearms (via a firearms licence) owned or used by Patients about whom there are, e.g. behavioural, concerns.

Health

When a person has a medical condition that puts others at risk, e.g. infection from a serious communicable disease such as HIV, and the Patient refuses to modify their behaviour or inform others.

5.7 Deceased Patients

The duty of confidentiality owed to deceased Patients

The ethical obligation to respect a Patient's confidentiality extends beyond death and a duty of confidence attaches to the medical records of the deceased under section 41 of the Freedom of Information Act.

The duty of confidentiality must be balanced with other considerations, e.g. the interests of justice and of people close to the deceased Patient. This requires Lister House Surgery to counsel Patients about possible disclosure after death where there may be sensitive issues with the content of discussions added to the clinical record.

Rights of access to a deceased Patient's records

Unless the Patient requested confidentiality whilst alive, a personal representative or anyone who may have a claim arising out of a Patient's death has a right of access to information directly relevant to the claim unless it may cause 'serious harm' to an individual, or if it relates to a third party other than a health professional.

Relatives' entitlement to information about the deceased Patient's last illness

There is very limited legal entitlement via Access to Health Records legislation with health professionals



principally using discretion to disclose information to a deceased Patient's relatives or others when there is a clear justification. Disclosure is likely to be what the deceased Patient would have wanted and may also be in the interests of justice or the balance of benefit to be gained by the disclosure to the family, e.g. of a hereditary condition.

From 1 August 2022, the last registered GP Practice is responsible for carrying out access to health record (AHR) requests for deceased individuals. Primary Care Support England (PCSE) will administer requests for Patients who have passed away and whose last registered GP Practice is now closed or they were unregistered at time of death.

5.8 Serious Communicable Diseases

Legal restrictions on disclosure

Serious communicable diseases such as HIV remain stigmatised health conditions and many Patients regard information about them as particularly sensitive and private. There is specific legislation covering the disclosure of information about serious communicable diseases as well as the common law duty of confidence and the Data Protection Act.

Disclosure of information to close sexual contacts

Every effort must be made to persuade Patients to agree to information being shared voluntarily and that, if they refuse to share the information, Lister House Surgery may be obliged to do so.

Disclosure of information where a health care worker has suffered a needlestick injury or other occupational exposure to blood or bodily fluids

Despite all reasonable precautions, there will be rare occasions where a health professional suffers a needlestick injury and the Patient is known by the treating doctor to have a blood-borne virus, e.g. HIV. Where the Patient is competent, consent must be sought to disclose the information but, where the Patient lacks capacity to consent to disclosure, it may only take place if it is in the best interests of the Patient, and legal advice will be required to assist with this assessment.

5.9 Information for Non-medical Purposes

Complaints

When a Patient makes a complaint, the complaint investigation will usually require access to the relevant parts of their health record making the use of identifiable information necessary and appropriate. Patients must be made aware of who will see information about them and the safeguards in place to minimise any risks to confidentiality.

When Patients involve others, e.g. their MP, in the complaints process and it is stated in writing that the Patient has given consent for disclosure this is usually acceptable, although proof of consent is advised. Only information relevant to the complaint must be disclosed to the third party and the Patient must be copied into the response.

Patients are entitled to authorise relatives or carers to act on their behalf. Lister House Surgery must be satisfied that the Patient has given valid consent before disclosing any confidential information.

5.10 Subject Access Requests

Patients have the right to see their medical records, the records held by Lister House Surgery of information relating to their physical and mental health. Medical records include everything from the clinical records made by Lister House Surgery in consultations and other contacts, e.g. phone calls and messages, to results of tests, scans, X-rays, hospital attendances and admissions and the content of outpatient appointments to which the Patient has been referred by Lister House Surgery and all previous GPs.

Lister House Surgery treats Patient medical records as highly confidential because they are personal, sensitive and up to date in line with all statutory confidentiality and data protection obligations. Lister House Surgery holds health records both electronically and in paper files in line with NHS requirements.

Patients can access their own health record by written (subject access) request to Andrew Smythe using the Subject Access Request form available from the Reception Team or the website of Lister House Surgery. Lister House Surgery will only consider making a charge for Subject Access Requests if they are repeated or unreasonable in size (as they are usually used to respond to one matter or issue and not to obtain a copy of a whole medical record).

5.11 Training

Data protection and information governance training will be available to all staff and must be completed annually.

5.12 Data Breaches

All information governance breaches, actual or suspected, will be reported to, and investigated by, Andrew



Smythe in conjunction with the Data Protection Officer.

5.13 Caldicott Guardian

Dr Andrew Brooks is the Caldicott Guardian at Lister House Surgery and is responsible for:

- Ensuring that Lister House Surgery satisfies the highest practical standards for handling Patient identifiable information
- Facilitating and enabling appropriate information sharing and making decisions on behalf of Lister House Surgery following advice on options for lawful and ethical processing of information, in particular, in relation to disclosures
- Representing and championing information governance requirements and issues at Lister House Surgery
- Ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff, and
- Overseeing all arrangements, protocols and procedures where confidential Patient information may be shared with external bodies

5.14 Senior Information Risk Owner (SIRO)

Andrew Smythe is nominated as the Senior Information Risk Owner (SIRO) for Lister House Surgery. The responsibilities of the SIRO are to:

- Take overall ownership of the organisation's Information Risk strategy
- Understand how the strategic business goals of Lister House Surgery and other organisations' business goals may be impacted by information risks, and how those risks may be managed
- Implement and lead the information governance risk assessment and management processes at Lister House Surgery
- Sign off and take accountability for risk-based decisions and reviews in regard to the processing of personal data
- Advise on the effectiveness of information risk management at Lister House Surgery, and
- Receive training as necessary to ensure they remain effective in their role as SIRO

5.15 Data Protection Officer (DPO)

Lister House Surgery must appoint a Data Protection Officer (DPO) Paul Couldrey who reports to the SIRO, but also can act independently of the SIRO and report directly to Dr William Mark Hale about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

The DPO will:

- Provide advice to Lister House Surgery and its employees on compliance obligations with data protection law
- Advise on when data protection impact assessments are required
- Monitor compliance with data protection law and organisational policies in relation to data protection law
- Co-operate with, and be the first point of contact for, the Information Commissioner
- Be the first point of contact within the organisation for all data protection matters
- Be available to be contacted directly by data subjects
- Take into account information risk when performing the above

5.16 Management Responsibilities

Andrew Smythe and all line managers must take responsibility for ensuring that this policy is implemented within their team.

5.17 Staff Responsibilities

It is the responsibility of each employee to adhere to this policy and all associated data protection and information governance policies and procedures at Lister House Surgery.

Staff may receive instruction and direction regarding the policy from several sources:

- Line Manager or Andrew Smythe
- DPO



Lister House Surgery
Dr Hale and Partners, 207 St Thomas Road, Derby, Derbyshire, DE23 8RJ

- Data Protection policy and procedures
- Specific training course
- Other communication methods, for example, team meetings; and
- Staff intranet

All staff are mandated to undertake mandatory information governance training in line with the training skills and training matrix at Lister House Surgery.

Information governance training is required to be undertaken on an annual basis by all staff.

All staff must make sure that they use the IT systems at Lister House Surgery appropriately and adhere to the data protection policies.

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc. of personal data, states it is an offence for a person knowingly or recklessly:

- To obtain or disclose personal data without the consent of the controller
- To procure the disclosure of personal data to another person without the consent of the controller, or
- After obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained



6. Definitions

6.1 Information Governance

- Information governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service
- It provides a consistent way for employees to deal with the many different information handling requirements including:
 - Information governance management
 - Clinical information assurance for safe patient care
 - Confidentiality and data protection assurance
 - Corporate information assurance
 - Information security assurance
 - Secondary use assurance
 - Respecting data subjects' rights regarding the processing of their personal data

6.2 Confidentiality: NHS Code of Practice

- This sets out the standards required for NHS organisations concerning Patient confidentiality

6.3 Public interest

- There is no definition of public interest (or of "harm") so that officials considering a request for information can conduct a specific analysis in light of the current circumstances rather than being constrained by set criteria. The balance of public interest in respect of the disclosure of a particular piece of information may change over time and factors for and against disclosure must be weighed in response to each request when it is received
- Public interest is not the same as what the public is interested in, public curiosity about a subject is not the same as the public interest favouring the release of information

6.4 Records Management Code of Practice for Health and Social Care

- This sets out what people working with or in NHS organisations in England need to do to manage records correctly. It is based on current legal requirements and professional best practice and was published on 20 July 2016 by the Information Governance Alliance (IGA)

6.5 Best interests decision

- The Mental Capacity Act sets out what you must consider when deciding what is in the best interests of your Patient. You take into account: past and present wishes and feelings; beliefs and values that may have influenced the decision being made, had the person had capacity; and other factors that the Patient would be likely to consider if they had capacity
- You must have objective reasons for any decision you make
- You must also be able to show that you considered all circumstances relevant to the decision in question

6.6 Code of Practice on Confidential Information

- This sets out good practice guidance for organisations collecting, analysing, publishing or otherwise disseminating confidential information concerning, or connected with, the provision of health services or adult social care in England published by the Health and Social Care Information Centre (December 2014)

6.7 Capacity

- 'Mental capacity' means being able to make your own decisions. Someone lacking capacity, because of an illness or disability such as a mental health problem, dementia or a learning disability, cannot do one or more of the following things: Understand information given to them about a particular decision, retain that information long enough to be able to make the decision, weigh up the information available to make the decision

6.8 DVLA

- The Driver and Vehicle Licensing Agency is the organisation of the UK government responsible for maintaining a database of drivers in Great Britain and a database of vehicles for the entire United Kingdom



6.9 GDPR

- The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas

6.10 Caldicott Guardian

- A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically and appropriately and that confidentiality is maintained

6.11 Data Protection Act 2018

- The Data Protection Act 2018 (c 12) is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation (GDPR) and updates the Data Protection Act 1998



Key Facts - Professionals

Professionals providing this service should be aware of the following:

- Maintaining confidentiality is a legal requirement that preserves the trust between Patients and healthcare professionals. This is a major factor in encouraging Patients to provide the information necessary to make sure they receive appropriate treatment and care
- Every piece of identifiable Patient information is confidential and must be treated as such while it exists, including when it is in the memory of any member of staff, according to the HSCIC code of practice on confidential information for health and social care
- When third parties request information about Patients or their treatment Patients must give their consent, be properly informed how the identifiable information about them will be used and assured that only relevant or necessary information will be disclosed
- Patients who are competent and able to make their own decisions are generally considered to have given their implied consent for the sharing of necessary information that is relevant for their health and care between health professionals on a confidential 'need to know' basis
- There are special provisions for sharing information about Patients who lack mental capacity, deceased Patients and children. It is reasonable to assume a Patient who lacks capacity would like information shared with the people closest to them unless there is contrary evidence or suggestion. Deceased Patients retain the duty of confidentiality in particular when they asked for information to remain confidential while they were alive. Children and young people are entitled to the same duty of confidentiality as to adults
- Where doubt exists about the disclosure of confidential Patient information an experienced or specialist healthcare professional or a Caldicott Guardian must be consulted and reasons for disclosure must be fully documented to justify the decision
- All members of staff are legally bound by a duty of confidentiality which is also recorded in their employment contract, contractors and other people working at Lister House Surgery are required to sign confidentiality agreements to preserve and safeguard Patient confidentiality
- Patients must be able to feel safe and expect information about them and their health that they give in confidence will be kept confidential and only shared with their prior consent, unless there is an entirely valid reason for it to be disclosed without their consent
- From 1 August 2022, the last registered GP Practice is responsible for carrying out access to health record (AHR) requests for deceased individuals



Key Facts - People affected by the service

People affected by this service should be aware of the following:

- As a Patient, you have the right to access your own medical records by a Subject Access Request which may be met by providing online access (where this is available), electronically (using encryption) or on paper. The surgery only needs to print paper copies if asked to do so and this is reasonable. If there is a large amount of information about you in your clinical record, the surgery can ask for clarification of the relevant information that would be acceptable to satisfy the Subject Access Request
- Confidentiality is essential to the doctor-patient relationship and this extends to everyone working at your surgery who may require access to some or all of your confidential Patient information for the purposes of your health, care and treatment, at all times and without exception
- Your consent to the sharing of personal information that relates to your health is implied, e.g. between healthcare practitioners and staff in respect of a hospital referral etc. All healthcare staff involved in providing patient care are bound by the duty of confidentiality. You can object to the sharing of your information, but your doctor or nurse may tell you it is not possible to provide you with the level of safe care you need without sharing your information, e.g. when referring you for treatment
- All identifiable Patient information in any form, e.g. medical records, photos, hospital letters and anything that can be used to identify you directly or indirectly, is confidential and must be treated as such while it exists. As well as the laws governing information, the NHS and professional bodies set very clear confidentiality standards and guidance on what constitutes a breach of the duty of confidentiality
- If information is required by a third party, e.g. for insurance, employment or benefits purposes, you will be asked for your written consent to authorise the sharing of information about you. Only relevant and factual information will be disclosed which means no relevant information can be concealed or withheld at your request. You will usually be offered a copy of the finished report unless there is any valid reason otherwise



Further Reading

As well as the information in the 'underpinning knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

NHS England and NHS Improvement - Information Governance Policy:

<https://www.england.nhs.uk/publication/information-governance-policy/>

CQC - Code of Practice on Confidential Personal Information:

<https://www.cqc.org.uk/sites/default/files/20180419%20Code%20of%20practice%20on%20CPI%20with%20GDPR%20and%20IRMER%20updates.pdf>

CQC - Confidentiality - Key Messages (for Inspectors):

<https://www.cqc.org.uk/sites/default/files/Confidentiality%20-%20Key%20messages.pdf>

National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs (2016):

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

NSPCC - Gillick Competency and Fraser guidelines:

<https://learning.nspcc.org.uk/research-resources/briefings/gillick-competency-and-fraser-guidelines/>

Please also refer to the QCS suite of Data Protection policies, including:

Data Security and Protection Policy and Procedure

Home Working Policy and Procedure

Record Keeping Policy and Procedure

Caldicott Guardian Policy and Procedure



Outstanding Practice

To be 'outstanding' in this policy area you could provide evidence that:

- Any member of staff working from home understands the importance of maintaining confidentiality when remotely accessing Patient data
- Every member of staff understands all the different requirements, aspects and implications of individual personal confidentiality, how they relate to mental capacity and to their duties and responsibilities in providing primary care for Patients, and when to consult a senior colleague or the Caldicott Guardian if there is doubt about disclosing or sharing Patient or other personal identifiable information that is required
- The wide understanding of the policy is enabled by proactive use of the QCS App
- Visitors and contractors work with Lister House Surgery in upholding the principles and abiding by the operational requirements of Patient and individual confidentiality and information security, and they enter into a confidentiality agreement in respect of the time they spend working on site at Lister House Surgery
- Patient confidentiality outside of the consulting room is managed by the administrative team, signed off by the responsible healthcare professional and overseen by the Caldicott Guardian; this ensures that skills and knowledge are used effectively and the Patient can remain at the centre, as far as the allocation of resources is concerned
- Everyone recognises and understands there is no difference between the duty of confidentiality that relates to Patients, to colleagues and to all other individuals whose personal identifiable information is available to Lister House Surgery. They are all owed the same duty of confidentiality and entitled to keep their personal identifiable information private unless they consent to its disclosure or there is a justifiable reason for it to be shared without their consent
- Sharing the information necessary for delivering effective healthcare for Patients in the community is supported by the relevant consent mechanisms and confidential communication systems that enable timely, integrated care to be provided by a multidisciplinary team who may be based in different premises in a wider locality to Lister House Surgery
- Fax machines are no longer used for the transfer of Patient identifiable confidential or Patient related clinical information and there are safe electronic systems and methods in place for the transmission of confidential Patient information that are paper light



Forms

The following forms are included as part of this policy:

Title of form	When would the form be used?	Created by
Confidentiality Agreement - GCP02	To ensure that staff understand their confidentiality obligations.	QCS

Lister House Surgery
Dr Hale and Partners, 207 St Thomas Road, Derby, Derbyshire, DE23 8RJ

This agreement is provided to clarify the responsibilities of those employed by Lister House Surgery in respect of maintaining confidentiality of the information collected and used in the course of and necessary for providing primary care to Patients.

Queries and questions relating to this duty must be addressed to Andrew Smythe in the first instance.

All Patient information is given on the understanding that it will be used solely in connection with providing care and treatment. It is the duty of Lister House Surgery to ensure that the confidentiality of that information is maintained within the boundaries of the law and is not disclosed or shared without the consent of the Patient unless circumstances dictate otherwise.

In the course of your work at Lister House Surgery, you will have access to personal identifiable confidential data concerning the medical or personal affairs of:

- Patients
- The whole Practice Team
- Associated health and care professionals

Unless acting on Lister House Surgery policy or following the direct instructions of Andrew Smythe or the Caldicott Guardian for the practice, personal identifiable confidential information must not be divulged or discussed except in the performance of normal duties. Breach of confidence, including the improper passing of computer data or electronic images, may result in disciplinary action, your dismissal and civil action against you for damages.

Personal identifiable information about Patients, employers and colleagues is strictly confidential and must not be disclosed or shared with anyone without their consent or without a valid purpose that can be justified before and after the disclosure. This obligation is unlimited. It remains in force before, during and after your employment at Lister House Surgery. Disclosures of confidential information or disclosures of any data of a personal identifiable nature can result in a criminal prosecution under the Data Protection Act 2018.

You must ensure that all Patient and other confidential information, which includes the use of computer screens, portable data devices and electronic and paper records, is never left where it can be seen by unauthorised people or anyone else who has no valid reason for access.

Computer screens must always be cleared when left unattended and you must ensure that you log out of computer systems, remove your password and smartcard. All computer and other passwords and logins must be kept confidential and never shared.

No unauthorised use of the internet or email is permitted at work other than for the purpose of carrying out the duties and responsibilities of your role and the activities necessary to provide Patient care and business support services.

I have read, understand and agree to the terms and conditions set out above:

Signature:

Date:

Name: