POLICY TITLE:	**Confidentiality**
Policy Number:	LE06
Version Number:	03
Date of Issue:	15/02/2023
Date of Review:	15/02/2026
Policy Owner:	Shardé Hurd, Solicitor, Group Data Protection Officer
Ratified by:	David Watts, Director of Risk Management
Responsible Signatory:	Shardé Hurd, Solicitor, Group Data Protection Officer
Outcome:	This policy: • Aims to ensure that service users, their families or representatives and colleagues are assured of confidentiality • Details the delegation of officers, such as Caldicott Guardian • Provides details on the safe and secure transfer of information • Aims to ensure all colleagues comply with the requirements of the Data Protection Act when dealing with service user or colleague personal information
Cross Reference:	IT02 IT Security IT07 Printing, Photocopying, Scanning and Faxing IT11 Information Transfers LE03 Data Protection LE05 Service User Information/Interview Requests from Police or Other External Agencies OP04 Incident Management, Reporting and Investigation OP05 Mental Capacity OP05.1 Gillick Competency to Consent in a Healthcare Setting OP06 Safeguarding Children OP08 Safeguarding Adults OP21 Whistleblowing (Protected Disclosure) OP22 Use of CCTV

EQUALITY AND DIVERSITY STATEMENT

Priory is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any protected characteristics (age, disability, gender identity and expression, marriage or civil partnership, pregnancy or maternity, race, religion or beliefs, sex, sexual orientation), and all will be treated with dignity and respect.

To ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, email LegalandComplianceHelpdesk@priorygroup.com.

CONFIDENTIALITY

1 INTRODUCTION

1.1 All colleagues are required to protect confidential information concerning service users and other colleagues obtained in the course of their work.

1.2 Personal data is covered by the Data Protection Act 2018 and any breaches of confidentiality will be treated as an incident. Therefore this policy must be read in conjunction with:
(a) LE03 Data Protection;
(b) IT07 Printing, Photocopying, Scanning and Faxing;
(c) OP04 Incident Management, Reporting and Investigation;
(d) Divisional policies on management of service user records.

2 AIMS

2.1 Patients, students, residents, their family or representatives and colleagues have the right to be assured that information given in confidence will only be used for the purpose for which it was given and will not be released to others without their permission. The death of a service user does not give the right to break confidentiality.

2.2 Confidentiality is to be respected at all times and general confidential information must only be shared to enhance care and only with the service users consent. Confidentiality may only be broken in exceptional circumstances and may only occur after very careful consideration by senior management (refer to LE03 Data Protection).

2.3 Colleagues should be aware of the over-riding duty to breach confidentiality where there is a potential risk of harm to the service user, another colleague or members of the public. Safeguarding matters are likely to fall into this category. (Refer to OP06 Safeguarding Children and OP08 Safeguarding Adults).

3 TRAINING

3.1 All colleagues who have access to confidential service user information will receive training in confidentiality issues, for both induction and refresher e-Learning modules courses via the Priory Academy.

4 CORPORATE GOVERNANCE

4.1 All colleagues, including contractors, should be subject to strict confidentiality obligations in their contracts. A confidentiality statement is included on all emails being sent to external recipients and is included on electronic service user records (e.g. CareNotes).

5 SECURITY

5.1 IT systems and policies should offer robust arrangements for managing access and sharing of service user identifying information according to agreed management protocols. This will include written documentation, IT system information and any confidential information kept on individual business systems such as mobile phones/laptops and any other media processing devices. All colleagues will read the policy, IT02 IT Security, before they are given an access login to the Priory network.

5.1.1 'Systems' also includes images captured on surveillance cameras such as CCTV, or digital cameras used for taking identification images on admission.

5.2 Colleagues must ensure that confidential hard copy records are kept in locked storage facilities and not accessible to unauthorised people at any time.

6 PROVIDING INFORMATION

6.1 It is important that the service user (and their family or representatives, if applicable) understands that some confidential information may be made available to others involved in the delivery of their care.

6.2 Confidentiality and its limits must be explained to service users and their carers on admission both verbally and in writing.

6.3 The issues of confidentiality and information sharing between mental health professionals and carers can be challenging but it is often crucial to the ongoing wellbeing of the patient and carers.

6.4 The service user (and their family or representatives, if applicable) is to be made aware with whom the confidential information will be shared and for what purpose it will be shared.

6.5 As far as is reasonable, confidential information is to be kept in strict professional confidence and be used only for the purposes for which the information was given.

6.6 Issues around confidentiality should not be used as a reason for not listening and talking to carers, nor for not discussing fully with our service users. The need for carers to receive information, is so they that they can continue to support them.

6.7 Other than in the limited circumstances stated in paragraphs 6.8 (b), 6.8 (c) and 6 (d) below, explicit consent from the service user is always required before confidential information is disclosed. If the service user does not have the capacity to give consent, a best interests decision must be in place (refer to OP05 Mental Capacity) prior to the sharing of any confidential information.

6.8 Disclosure of confidential information is permitted:

(a) With the consent of the service user.
(b) If life is in danger (to self or others) then the general principles of confidentiality no longer applies and family or representatives will be informed immediately if their loved one becomes very ill whilst in our care. Emergency services may also be informed in circumstances where life is in danger.
(c) Without the consent of the service user when the disclosure is permitted by law or by order of a court.
(d) Without the consent of the service user when the disclosure is considered to be necessary in the public interest.

6.9 Disclosing information in the public interest means the interest of an individual or groups of individuals or of society as a whole, and would, for example, cover matters such as serious crime, drug trafficking or other activities, which places others at serious risk.

6.10 Colleagues are responsible and accountable for any decision they make to release confidential information.

6.11 Colleagues are not to deliberately breach confidentiality other than in the exceptional circumstances noted in paragraphs 6.8(b), 6 (c) and 6.8(d).

6.12 Any enquiries from the press, radio or television will be referred immediately to the site/service/departmental manager.

6.13 The private addresses or phone numbers of individuals should not be included in service user documentation or reports, unless it is expressly required for the function of that documentation.

6.14 Failure to comply with this policy will result in disciplinary action.

7 CONFIDENTIALITY AND THE YOUNG PERSON

7.1 Data subjects have the same data protection rights regardless of age. Both the BMA and GMC expressly state that the duty of confidentiality owed to a young person is as great as the duty owed to any other person.

7.1.1 If a child or young person does not agree to disclosure of confidential information there are still circumstances in which disclose can take place:
(a) When there is an overriding public interest in the disclosure.
(b) When disclosure is in the best interests of a child or young person who does not have the maturity or understanding to make a decision about disclosure.
(c) When disclosure is required by law.

7.1.2 In respect of 7.1.1(b) above, young people aged 16-17, and younger people under 16 who are Gillick competent are considered to have the maturity to understand the decision regarding disclosure and are entitled to have their confidence respected. (Refer to OP05.1 Gillick Competency to Consent in a Healthcare setting).

7.2 A child can be regarded as Gillick competent if the doctor concludes that they has the capacity to make the decision that needs to be made at that particular time and has sufficient understanding and intelligence to be capable of making up their own mind. (Established in Gillick v West Norfolk and Wisbeach Area Health Authority (1986)).

7.3 In safeguarding cases if sharing information is essential to safeguard a child's welfare, it would satisfy the "overriding public interest" threshold.

8 CALDICOTT PRINCIPLES

8.1 Dame Fiona Caldicott led an in depth Information Governance Review in 2013 of the well-established Caldicott Principles for the maintaining the confidentiality of Health and Social Care records, leading to an updated set of seven principles (see **Appendix 1**).

8.2 The review also lays out a set of five confidentiality rules which must be followed by all colleagues having access to personal confidential data:
(a) Confidential information about service users should be treated confidentially and respectfully.
(b) Members of a care team should share confidential information when it is needed for the safe effective care of a service user.
(c) Information that is shared for the benefit of the community should be anonymised.
(d) An individual's right to object to the sharing of confidential information about them should be respected.
(e) Organisations should put policies, procedures and systems in place to ensure that the confidentiality rules are followed.

9 DELEGATION OF OFFICERS

9.1 The role of the Caldicott Guardian is a strategic role of representing confidentiality and security arrangements in respect of service user records at Operating Board level. Within the Priory Group this registered position is held by the Group Medical Director.

9.2 At site level, the duties of the Caldicott Guardian are delegated from the Group Medical Director to the site/service managers.

9.3 Colleagues should be advised to seek assistance from the person with delegated responsibility from the Caldicott Guardian and the Data Protection Team (personaldata@priory.com) where necessary. Typical examples of such situations are:
(a) A request from the police for access to service user information (also refer to LE05 Service User Information/Interview Requests from Police or Other External Agencies).

(b) Requests from service users to delete their records.
(c) An actual or alleged breach of confidentiality.

9.4 Refer to LE03 Data Protection for information regarding the Group Data Protection Officer for Priory Group.

10 COLLEAGUE CONFIDENTIALITY

10.1 Colleagues have a responsibility to ensure confidentiality when dealing with professional issues or complaints relating to another colleague.

10.2 Managers should ensure sensitivity and confidentiality to the colleague involved in any issue or complaint, where possible and appropriate.

10.3 The private addresses or phone numbers of colleagues should not be included in service user documentation or reports.

11 SECURE & SAFE TRANSFER OF CONFIDENTIAL INFORMATION (SAFE HAVEN)

11.1 The term 'Safe Haven' describes the administrative arrangements to safeguard the confidential transfer of service users' identifiable information between organisations or sites. It covers data held on:
(a) Fax machines.
(b) Answerphones.
(c) Photocopiers, printers.
(d) Computers, laptops, mobile phones.
(e) Message books.
(f) Post trays, including unopened post.
(g) Visitor books.
(h) Dictation equipment.

11.1.1 Reference should be made to IT11 Information Transfers when transferring data electronically.

11.2 When information is disclosed by a designated safe-haven point to an equivalent point in another organisation, colleagues can be confident that agreed protocols will govern the use of the information from that point on.

11.3 A system of secure email transfers of confidential information between Priory units and the NHS became operational from February 2009. This has strict controls and a local procedure documenting usage that must be in place on each site.

11.4 Responsibility for maintaining the confidentiality of service users' identifiable information lies with the site/service manager or the departmental manager for central service functions. Individual colleagues are responsible for ensuring that the procedures are always applied when transferring confidential data between organisations and must at all times comply with LE03 Data Protection Policy.

11.5 **Printers, Photocopiers, Scanners and Fax Machines** - Refer to IT07 Printing, Photocopying, Scanning and Faxing for guidance on maintaining confidentiality of this equipment.

11.6 **Post** - Post should be opened in an area away from service users and visitors. Post in and out trays must be sited away from the general public and stored in an area with controlled access.

11.7 **Message Books, Appointment Books etc. -** Written records must be sited away from the general public and at the end of each session must be stored in a secure location.

11.8 **Computers, Email and Mobile Phones** - Service user's identifiable information must not be sent by email apart from authorised use of the secure 'NHS Mail' web-based email system, controlled centrally. However, there will occasionally be instances where it is appropriate to use a service user's name rather than initials in email communication, for example when corresponding with family.

11.8.1 Computer screens must be away from the sight of visitors and the general public. This includes views from ground floor windows. Users of computer systems must log out of all application systems before leaving a PC unattended. Refer to IT02 IT Security.

11.8.2 The use of personal mobile phones or cameras to take photographs of service users is not permitted.

11.9 **Other Electronic Media** - Dictation equipment containing personal information should always be kept in a locked area when not in use. They should be cleared of all dictation when the communication has been completed. There must be an area available for colleagues to use the phone away from public areas and photocopiers/printers should be sited in areas where there is no access for the public and service users.

12 FILMING, PHOTOGRAPHY OR VIDEO

12.1 Unless expressly authorised in advance by a site leader or other senior manager for purposes strictly connected with work, colleagues are not permitted to take pictures, film or record footage (using phones or other recording equipment) of service users or other colleagues whilst at work.

12.1.1 This also applies to covert filming. If a colleague has concerns about the care or treatment of a service user, this must be reported to line management or via the whistleblowing helpline/mailbox Whistleblowing@priorygroup.com in accordance with OP21 Whistleblowing (Protected Disclosure).

12.2 Anyone found taking pictures or recording footage of service users or colleagues either overtly or covertly, without the express permission of senior management for a legitimate work purpose (such as supervision or training) will be dismissed for gross misconduct. The matter is likely to be notified to the police, the Information Commissioner's Office (ICO) and relevant regulatory, safeguarding and professional bodies.

13 USING GENUINE CASE STUDIES

13.1 All information that relates to a living person is subject to the requirements of the Data Protection Act 2018 (refer to LE03 Data Protection). These guidelines must be followed if case studies of service users or colleagues containing such information are used externally for publicity, marketing, tendering or for any other reason.

13.2 All materials intended for external use/general publication/public media must be approved in writing by the central Communications team before use. The Communications team will check that appropriate consents and safeguards are in place to ensure that the requirements of the Data Protection Act are not breached, for example:

(a) Articles do not contain the service user's/colleague's real name.
(b) Service Users and/or colleagues have consented to the use of photographs. (If the service use lacks capacity to consent, photographs of them must not be used)
(c) Other details about colleagues and/or service users do not identify the subject as a specific person.

13.3 Case studies for restricted external use (e.g. tenders and proposals) should be sourced in the first instance from Top Priority or from the Communications team, as these will already have been checked to make sure the appropriate consents or safeguards are in place.

14 REFERENCES

14.1 Legislation

Data Protection Act 2018
Health and Social Care Act 2012, Section 265

14.2 Guidance

DH (2003) Confidentiality: NHS Code of Practice
DH (2013) Information: To share or not to share. Government response to the Caldicott Review
Health and Social Care Information Centre (2013) A Guide to Confidentiality in Health and Social Care: Treating confidential information with respect
NMC (2015) The Code: Professional standards of practice and behaviour for nurses and midwives (updated 2018)
UK Caldicott Guardian Council (2017) A Manual for Caldicott Guardians
DHSSPSNI (2011) Residential Care Homes Minimum Standards
DHSSPSNI (2015) Care Standards for Nursing Homes
Scottish Government (2018) Health and Social Care Standards: My support, my life
Welsh Assembly Government (2002) National Minimum Standards for Care Homes for Younger Adults
Welsh Assembly Government (2004) National Minimum Standards for Care Homes for Older People
Gillick v West Norfolk and Wisbech Area Health Authority [1985] 3 All ER 402

Appendix 1 – The Caldicott Principles

Appendix 1

TO SHARE OR NOT TO SHARE
The Caldicott Principles

(Adapted for Priory from 'A Guide to Confidentiality in Health and Social Care (HSCIC) 2013)

1. **Justify the purpose(s)** – Every proposed use or transfer of personal confidential data within or from a Priory site should be clearly defined scrutinised and documented, with continuing uses regularly reviewed, by the person in charge of the site.

2. **Don't use personal confidential data unless it is absolutely necessary** – Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for service users to be indentified should be considered at each stage of satisfying the purpose(s)

3. **Use the minimum necessary personal confidential data** – Where use of personal confidential data is considered to be essential the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out

4. **Access to personal confidential data should be on a strict need to know basis** – Only those individuals who need access to personal confidential data should have access to it, and then should only have access to the data items that then need to see.

5. **Everyone with access to personal confidential data should be aware of their responsibilities** – Action should be taken to ensure that colleagues handling personal confidential data, (which means all colleagues, whether clinical, non-clinical or office colleagues) are made fully aware of their responsibilities and obligations to respect service user confidentiality.

6. **Comply with the Law** – Every use of personal confidential data must be lawful. The Caldicott Guardian is responsible for ensuring that Priory complies with legal requirements, and it is the responsibility of every colleague to ensure that they comply with the requirements set out in Priory policy, and use the systems and processes put in place correctly.

7. **The duty to share information can be as important as the duty to protect service user confidentiality** – All Priory colleagues should have the confidence to share information in the best interests of their service users with the framework set out by these principles. They are supported by the policies of the regulatory and professional bodies and by Priory policies (both corporate and divisional).