Medicare People

LIVE-IN CARE

Data Protection and Confidentiality Policy and Procedure

Policy Title	Data Protection and Confidentiality Policy and Procedure
Organisation	Medicare People Limited
Service Type	Live-In Care Services
Policy Owner	Registered Manager
Version	1.0
Date Created	07/07/2026
Review Date	Annually

1. PURPOSE

Medicare People is committed to protecting the privacy, confidentiality, integrity, and security of personal information held about individuals receiving care, employees, representatives, and others associated with our services.

The purpose of this policy is to establish clear standards for the collection, use, storage, sharing, retention, and disposal of personal information and confidential records.

This policy supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the common law duty of confidentiality, whilst ensuring that information is available where needed to provide safe and effective care.

2. Scope

This policy applies to:

- All employees, workers, agency staff, and contractors.
- All personal and confidential information processed by Medicare People.
- Paper and electronic records.
- Information relating to individuals receiving care and support.
- Employee records.
- Business and operational records.

This policy applies to all information obtained, created, stored, shared, or disposed of during the course of Medicare People's activities.

3. Definitions

Personal Data — Any information relating to an identified or identifiable individual. Examples include:

- Name
- Address
- Date of birth
- Contact details
- NHS number
- Care records

Special Category Data — Personal information requiring additional protection, including information relating to:

- Health
- Race or ethnicity
- Religious beliefs
- Sexual orientation
- Biometric data

Confidential Information — Information provided in confidence or information that should reasonably be expected to remain private.

Processing — Any activity involving personal information including:

- Collection
- Recording
- Storage
- Viewing
- Updating
- Sharing
- Disposal
- Data Subject
- The individual to whom personal data relates.

Data Breach — A security incident that results in the unauthorised access, disclosure, loss, destruction, or alteration of personal information.

4. Policy Statement

Medicare People will:

- Process personal information lawfully, fairly, and transparently.
- Collect only information that is necessary for legitimate purposes.
- Maintain accurate and up-to-date records.
- Protect information against loss, theft, misuse, or unauthorised access.
- Respect the confidentiality of individuals receiving care and support.
- Ensure information is only shared when lawful and appropriate.
- Comply with all relevant data protection legislation.
- Provide employees with appropriate training and guidance.
- Investigate and manage data breaches promptly.
- Promote a culture of confidentiality and information security.

All employees have a responsibility to protect the information they access as part of their role.

5. Roles and Responsibilities

Registered Manager

The Registered Manager is responsible for:

- Ensuring compliance with data protection legislation.
- Monitoring information governance arrangements.
- Investigating data protection breaches.
- Ensuring secure information storage and disposal.
- Supporting employees with information governance matters.
- Maintaining oversight of information security risks.

Care Coordinators and Assessors

Care Coordinators and Assessors are responsible for:

- Maintaining accurate records.
- Sharing information appropriately.
- Protecting confidential information.
- Reporting concerns regarding data security.

Live-In Carers

Live-In Carers are responsible for:

- Maintaining confidentiality.
- Protecting records and information.
- Recording information accurately.
- Reporting actual or suspected data breaches.
- Following organisational procedures regarding information sharing.

All Employees

All employees must:

- Comply with this policy.
- Protect confidential information.
- Access information only when authorised.
- Follow data protection requirements.
- Report breaches and concerns immediately.
- Complete mandatory training.

---

6. Procedure

6.1 Collecting Information

Medicare People will only collect information that is:

- Relevant.
- Necessary.
- Accurate.
- Required to provide care, manage employment, or meet legal obligations.

Information should normally be obtained directly from the individual wherever possible.

6.2 Lawful Processing of Information

Personal information will only be processed where there is a lawful basis to do so.

This may include:

- Consent.
- Performance of a contract.
- Compliance with legal obligations.
- Protection of vital interests.
- Legitimate organisational interests.
- Provision of health and social care services.

Employees must ensure information is only used for legitimate business purposes.

6.3 Confidentiality

All confidential information must be treated with respect and discretion.

Employees must:

- Avoid discussing confidential information in public areas.
- Ensure records are not accessible to unauthorised individuals.
- Verify identity before sharing information.
- Respect the privacy of individuals receiving care.
- Follow the principle of sharing only information that is necessary.

Confidentiality obligations continue after employment ends.

6.4 Access to Information

Access to personal information will be restricted to individuals who require it to perform their duties.

Employees must:

- Only access records relevant to their role.
- Never access information out of curiosity.
- Never share passwords or security credentials.
- Log out of systems when not in use.

Unauthorised access may result in disciplinary action.

6.5 Information Sharing

Information may be shared where:

- Consent has been obtained.
- There is a legal requirement.
- There is a safeguarding concern.
- Disclosure is necessary to prevent serious harm.
- Sharing is required to support care delivery.

Information sharing should always be:

- Necessary.
- Proportionate.
- Relevant.
- Secure.

Where possible, individuals should be informed when information is shared.

6.6 Storing Information

Personal information must be stored securely.

This may include:

- Paper Records
- Locked cabinets.
- Restricted access areas.
- Secure transportation arrangements.
- Electronic Records
- Password protection.
- User access controls.
- Secure networks.
- Encryption where appropriate.

- Secure backups.

Appropriate security measures must be maintained at all times.

6.7 Using Mobile Devices

Employees using laptops, tablets, or mobile phones for work purposes must:

- Keep devices secure.
- Use passwords or biometric protection.
- Prevent unauthorised access.
- Report lost or stolen devices immediately.
- Avoid storing unnecessary personal information on devices.

Confidential information must never be left visible or unattended.

6.8 Subject Access Requests

Individuals have the right to request access to personal information held about them.

Any Subject Access Request must be forwarded immediately to the Registered Manager.

Requests will be managed in accordance with applicable legislation and organisational procedures.

6.9 Data Breaches

Any actual or suspected data breach must be reported immediately.

Examples include:

- Lost records.
- Misdirected emails.
- Incorrect disclosure of information.
- Lost devices.
- Cybersecurity incidents.
- Unauthorised access to records.

The Registered Manager will:

- Assess the breach.
- Take action to limit harm.
- Investigate the incident.
- Determine reporting obligations.
- Implement corrective actions.

All breaches will be recorded.

6.10 Retention and Disposal of Records

Records will be retained in accordance with legal and organisational requirements.

When records are no longer required they will be disposed of securely.

Approved disposal methods may include:

- Confidential shredding.
- Secure destruction services.
- Permanent electronic deletion.

Confidential information must never be discarded through general waste systems.

6.11 Confidentiality in Live-In Care Settings

Employees working within individuals' homes must be particularly mindful of confidentiality.

Employees must:

- Respect private information heard or observed within the home.
- Avoid discussing one service user with another.
- Ensure care records are stored safely within the home where applicable.
- Respect the privacy of family members and visitors.
- Only share information relevant to care delivery and safety.

The individual's home should be treated with the same confidentiality standards expected within healthcare settings.

---

7. Records and Documentation

The following records may be maintained:

- Care records.
- Care plans.
- Risk assessments.
- Consent records.
- Capacity assessments.
- Employee records.
- Training records.
- Subject Access Requests.
- Data breach reports.
- Audit reports.
- Information sharing records.
- Complaints records.

Records must be maintained securely and accessed only by authorised individuals.

---

8. Training and Competency

All employees will receive training covering:

- UK GDPR.

- Data Protection Act 2018.
- Confidentiality responsibilities.
- Information governance.
- Secure information handling.
- Data breach reporting.
- Information sharing principles.

Competency will be monitored through:

- Supervision.
- Audits.
- Observations.
- Appraisals.
- Training assessments.

Refresher training will be provided regularly.

9. Monitoring and Governance

The Registered Manager will monitor compliance through:

- Record keeping audits.
- Data protection audits.
- Data breach reviews.
- Complaints analysis.
- Staff supervision.
- Training compliance monitoring.
- Information governance reviews.

Key performance indicators may include:

- Data breach incidents.
- Audit compliance scores.
- Subject Access Request response times.
- Training completion rates.
- Corrective action completion rates.
- Complaints relating to confidentiality.

Learning identified through audits, incidents, complaints, and investigations will be used to strengthen information governance and service quality.

10. Related Policies

- Record Keeping Policy and Procedure
- Care Planning Policy and Procedure

- Consent to Care and Support Policy and Procedure
- Mental Capacity Act and Best Interests Policy and Procedure
- Safeguarding Adults Policy and Procedure
- Incident Reporting Policy and Procedure
- Medicines Management and Prescribing Policy and Procedure
- Whistleblowing Policy and Procedure
- Quality Assurance Policy and Procedure
- Equality, Diversity and Human Rights Policy and Procedure

---

11. Review and Version Control

This policy will be reviewed annually or sooner following:

- Changes in legislation.
- Changes in regulatory guidance.
- Data breaches.
- Audit findings.
- CQC inspection outcomes.
- Service developments.

Approved By: Stuart Wells

Position: Managing Director

Date: 07/07/2026

Medicare People currently provides introductory live-in care services. We have submitted our application to the Care Quality Commission (CQC) and intend to introduce a fully managed live-in care service following registration.