Standard Operating Procedure (SOP) for the Use of Leicester, Leicestershire and Rutland Care Record (LLR CR)

Owner	LLR Care Record Programme Manager, lpt.llrcarerecord@nhs.net
Version	1.0
Approval	LLR CR Adoption and Safety Group, 9 January 2024
Review	9 January 2025

Objective: The objective of this Standard Operating Procedure (SOP) is to establish guidelines for the proper and secure use of the Leicester, Leicestershire and Rutland Care Record (LLR CR) to ensure accurate, efficient, and collaborative health and care delivery.

Scope: This SOP applies to all health and care professionals, administrators, and support staff who have access to the LLR CR.

Responsibilities

1. Health and Care Professionals:
    - Integrate the LLR CR into local SOPs as required for consistent, sustainable and safe use, including consideration of business continuity.
    - Access the LLR CR using contextual launch through their native local system, or via the portal with their unique and secure credentials, as determined by their organisation.
    - Use the LLR CR only for legitimate and authorised direct healthcare purposes.
    - Keep login credentials confidential and report any suspected unauthorised access immediately in line with the LLR CR Information Sharing Agreement.
    - Report any discrepancies or issues with the LLR CR to the system administrator.
    - Misuse will be subject to disciplinary action by the manager of the staff member concerned and may also be subject to criminal prosecution.

2. System Administrators (Programme Team during transition):
    - Ensure the proper setup and maintenance of the LLR CR.
    - Grant and manage user access permissions based on roles and responsibilities, including prompt removal of access in the event of staff departure or transfer.
    - Monitor system activity to identify any unauthorised access or breaches.

3. System developers and testers:
    - Access the LLR CR using contextual launch through their native local system, or via the portal with their unique and secure credentials.
    - Keep login credentials confidential and report any suspected unauthorised access or other data protection incident.

4. Clinical safety and information governance assurance leads:

- Inform, shape and apply LLR CR assurance to minimise risk and in line with the requirements of the Integrated Care System (ICS) and its stakeholders.

5. The LLR CR Programme Team (transitioning to LLR CR platform owner):
    - Manage and develop the LLR CR on behalf of the LLR ICS under direction from the representative LLR CR Board.
    - Lead and coordinate LLR CR clinical safety and information governance assurance, involving all stakeholder organisations.
    - Maximise LLR CR availability and cascade key events and changes including new functionality and data releases to enable benefits, and incidents and downtime for business continuity.

Access and Authentication

1. User Authentication
    - Users accessing direct to portal must authenticate themselves using unique usernames, strong passwords and multi-factor authentication (MFA), or will be authenticated via Active Directory (AD).
    - Users accessing via contextual launch will have their access authorised via their native system.

2. Role-Based Access Control (RBAC)
    - Access permissions should be assigned based on the user's role to ensure they only access information necessary for their duties.

Data and Accuracy

1. Data timeliness and accuracy
    - The LLR CR is a read-only system.
    - Information should be entered promptly, clearly and accurately into native systems to ensure the LLR CR provides real-time and up-to-date information for patient care.

2. Clinical responsibility
    - Clinical responsibility for acting on indicators of concern originating from a single provider has been agreed to remain with the originators of the relevant information.
    - If information in combination from multiple providers raises new clinical, care or safeguarding concerns, the LLR CR user must follow up as dictated by their duty of care.

Security and Confidentiality

1. Encryption
    - All data transmitted using the LLR CR is secure and penetration testing is conducted routinely.

2. Audit Trails
    - The LLR CR maintains detailed audit trails to track user activity.
    - Forensic auditing will identify suspected improper use of LLR CR and privacy officers will be notified for investigation.

3. Confidentiality

- Users must protect and respect patient confidentiality and refrain from discussing patient information outside of the authorised healthcare context.

Incident Reporting

1. Security Incidents

- Any suspected security incidents, unauthorised access, or breaches must be reported to the system administrator immediately.

2.Data Integrity Issues

- Any issues related to data integrity or inaccuracies in the LLR CR must be reported promptly to the data provider organisation.

Training and Awareness

1. User Training

- All users should receive training on the proper use of the shared care record system and adherence to data protection and security protocols. LLR CR should be included in induction to maintain this.

2. Regular Updates

- Regular updates and refresher training sessions are available to ensure users are aware of any changes in procedures or system functionalities. Users can also access self-directed learning via the help button in the LLR CR.

Review and Compliance

1. Regular Audits

- Organisations are recommended to conduct regular audits of user access and system logs to ensure compliance with security policies.
- The required LLR CR usage data can be requested via the LLR CR Programme Team.

2. Policy Updates

- This SOP will be periodically reviewed and updated to reflect changes in technology, regulations, or organisational policies.
- Local SOPs should be amended by their owners where appropriate to remain in sync.

Document Control

1. Version Control

- The LLR Programme Team will maintain version control of this SOP to track changes and ensure that all users are aware of the latest procedures.

2. Distribution

- The LLR Programme Team will distribute the SOP to relevant personnel and ensure that it is readily accessible.

3. Approval

- This SOP was approved by the LLR CR Adoption and Safety Group on 9 January 2024.

4. Review Date:

- This SOP will be reviewed annually or as needed, with updates made as necessary to reflect changes in technology, regulations, or organisational policies.