CurrentCare® Operating Policy Overview

This document contains an overview of CurrentCare policies regarding the operation and use of CurrentCare Services. In order to share or access CurrentCare data, participating organizations ("participants") are required to complete the appropriate legal agreements, and onboarding forms and processes.

Key terms used in this document:

CurrentCare: Rhode Island's statewide Health Information Exchange (HIE).

The Rhode Island Quality Institute (RIQI) – riqi.org: the State of RI's Regional Health Information Organization (RHIO).

CRISP Shared Services (CSS) – CRISPsharedservices.org: the technology vendor ("Tech Vendor") for the State of RI's Health Information Exchange (HIE).

Participants: Participating organizations are required to adhere to the requirements in this CurrentCare Policy Overview, as well as share this policy overview with their authorized users. Updates to this document will be provided at: CurrentCareRI.org/Policies.

Users: Participant-authorized users are employees or other authorized individuals at participating organizations who are given access to CurrentCare services.

HIE Administrators ("HIE Admins"): Users authorized by participant organizations to manage all user access to CurrentCare.

Table of Contents

1. User Responsibilities

Participating organizations ("participants") may grant access to CurrentCare Services to their participating **users** (employees or other individuals whose job functions necessitate such access).

When organizations give their users access to CurrentCare Services, each user will be assigned a unique username and password. If a user works at multiple organizations, they will be assigned a unique username and password for **each** participating organization who assigns them access.

Each organization is responsible for having clear policies that describe how their authorized users must follow the CurrentCare policies outlined in this document. Organizations must also make sure their users follow all relevant laws, including HIPAA, and the terms of their agreement(s). If a user breaks any of these rules, the organization must notify CurrentCare immediately. CurrentCare may decide to pause or stop that user's access if needed.

1.1 Change in User's Job Status or Role

When a user's job status or role changes within a participating organization, if such change affects their access rights to the CurrentCare Services, HIE Administrators must promptly:

- **Change or remove the user's access/account**
- With each employee offboarding, HIE Admins should **assess if the user had access to MFT/SFTP** to upload or receive secure files. If that service needs to be terminated, the HIE Admin should promptly notify CurrentCare.

Participating organizations accessing CurrentCare Services through third- party EHRs, via SSO/SAML, will be responsible for terminating access through the EHR for the terminated user at the time of termination.

1.2 Training

CurrentCare has made training materials available online at: CurrentCareRI.org/training. Organizations are responsible for training individual users on data use and CurrentCare policies, including any updated training materials provided by CurrentCare.

If additional training is necessary because of system updates, CurrentCare will provide training resources and inform organizations of the changes, and each organization will then be responsible for training all its users.

2. User Authentication

CurrentCare uses secure industry standards for authenticating user access to CurrentCare Services and tools. CurrentCare and participating organizations must ensure that each user is assigned a unique username and password and that multi factor authentication (MFA) is enabled on each account to access the CurrentCare Services and tools.

2.1 Password Requirements & Expiration

CurrentCare password requirements differ across the tools and services. CurrentCare will communicate requirements as needed for each CurrentCare Service and tool.
User passwords will expire every 90 days, requiring that each user select a new password at that time. Password history settings will be enforced to ensure that a user does not duplicate a previously used password.

2.2 Lock Outs and Password Resets

Lockout: If a user has five (5) consecutive failed login attempts, their account will be locked. The user will need to wait at least 30 minutes before trying again. They will be required to change their password on the next login.

Reset: Users will be able to reset their password by clicking the "Reset your password?" option on the CurrentCare Portal login page: https://portal.CurrentCareRI.org. Alternatively, HIE Administrators at each organization can reset user passwords.

User Tip: CurrentCare Portal users can view a list of their HIE Admins using the "My HIE Admin(s)" button at the top of Portal. When users first get access to the Portal, they should make note of the names of their HIE Admins.

Suspended Account: CurrentCare automatically suspends user accounts for two reasons:

- HIE Admin didn't perform an audit of account within 90 days
- User didn't login within 90 days

For users who have been **suspended** but continue to need access, HIE Admins can **reactivate** their account. If accounts are not reactivated by 120 days, they will automatically be **deactivated**.

3. User Access Policies

All participating organizations are required to develop, or have in place, policies that govern how the organization and their users access information systems (such as CurrentCare) and use protected health information. Such policies should be consistent with the permitted purposes in the agreements and this CurrentCare Policy Overview and should be made available to CurrentCare upon request.

HIE Admins: Organizations must appoint authorized individuals to manage access at their organization to CurrentCare and its data. HIE Admin resources and responsibilities are available at CurrentCareRI.org/hie-admin.

Compliance: Organizations must appoint an authorized individual to implement and ensure compliance with all policies related to CurrentCare Participant Users. The authorized individual will be responsible for implementing a policy that appropriately grants users access to clinical data on behalf of the organization. This authorized individual may also act as the designated point of contact for CurrentCare correspondence and user verification and updates, as described in Section 8 (Audit).

3.1 Data Misuse

Health information available through CurrentCare is to be accessed, viewed, and used only by authorized CurrentCare participant organizations and their authorized users, and only for permitted purposes. CurrentCare uses a privacy tool for additional monitoring of all user activities regarding protected health information access to ensure all provisioned accounts are being used appropriately and to protect the confidentiality of protected health information; however, it is ultimately the participant organization's obligation to ensure the appropriate use of CurrentCare services by the organization and its users.

Any actual or suspected misuse of protected health information in connection with CurrentCare services must be reported to CurrentCare as soon as discovered. The actual or suspected misuse of protected health information will be investigated by CurrentCare and the participating organization. CurrentCare will notify privacy and security officers of all impacted parties at the conclusion of such investigations, if it is determined that a misuse of protected health information has occurred. As appropriate, CurrentCare and/or the organization will also take actions necessary to remedy the misuse of data. These actions may include, but are not limited to, suspension and/or modification of access privileges for an organization or its user(s).

3.2 Participant Procedures for Non-Compliance

In accordance with the Agreements, each participant organization should implement procedures to mitigateand deter misuse and issue appropriate consequences to hold their users accountable for misuse of data obtained when accessing protected health information through CurrentCare Services. As applicable, procedures in place for use of other health information systems may be leveraged to satisfy the requirements of this Section 3.2.

3.3 Third Parties

Participating organizations may have relationships with unaffiliated third parties whereby that third party sends, receives, or uses CurrentCare data or services via access granted by the organization. Organizations are responsible for having valid and enforceable agreements with each of its third parties that require the third party to, at a minimum: (i) comply with all Applicable Laws and Standards; (ii) comply with the terms of the Agreement as applicable including but not limited to protecting the privacy and security of any data to which it has access; (iii) refrain from disclosing to any other person any passwords or other access credentials issued to the third party by the participating organization; and (iv) comply with the relevant sections of this CurrentCare Policy Overview, including, but not limited to Sections 3.1, 3.2, and 3.3, as applicable.

4. Permitted Purposes

"Permitted Purpose" shall mean any one of the following reasons for which Message Content containing Patient Participant PHI can be Disclosed:

1. Treatment, Payment, and Authorization based disclosures as those capitalized terms are defined by HIPAA;

2. Transaction of Message Content related to value-based payment models, alternative payment arrangements or financial risk sharing models of any nature whether for Medicare, Medicaid, other federal programs, commercial payers or employer self-insured arrangements; to the extent permitted under the Information Privacy and Protection Laws;

3. Transaction of Message Content for public health activities and reporting permitted under R.I.G.L. § 5-37.7 and the Information Privacy and Protection Laws with

documented authority from a public health authority that are necessary to allow a public health authority to identify, monitor, assess, or investigate potential public health signals, onsets of disease outbreaks, or conditions of public health importance (including trends, signals, risk factors, patterns in diseases, or increases in injuries from using consumer products); and/or

4. Transaction of Message Content in support of an individual's: (i) right to access their health information or (ii) right to direct or restrict with whom their information can be shared or where their information should be sent.

5. Data Retention

CurrentCare will retain disclosure data for a minimum period of seven (7) years in order to maintain an auditable history of each transaction through CurrentCare Services. In addition, CurrentCare will retain copies of all its policies and procedures, all complaints received and resolved by CurrentCare, all Breach and potential Breach investigations undertaken by CurrentCare, all agreements with Participants and DSPs, Business Associates, and other third-parties, for a minimum period of seven (7) years.

6. Systems Operations

CurrentCare uses robust security measures, including encryption and access controls, to protect the confidentiality, integrity, and availability of patient data in compliance with relevant regulations such as HIPAA. Comprehensive data backup and disaster recovery plans are in place and regularly tested to ensure business continuity and minimize potential data loss in the event of system disruptions.

CurrentCare follows the strictest standards in healthcare technology security, including:

- Consistent system checks & network monitoring
- State-of-the-art monitoring tools
- Routine technology penetration testing
- Next-generation audit capabilities
- Strong encryption to protect your data
- Secure access controls and multi-factor authentication

6.1 Maintenance

Participants will be required to provide CurrentCare with at least one, but highly recommend two, **Support Contacts**. Participant support contacts will be expected to assist with issues surrounding on-going training, master patient index (MPI) administration, data quality, system upgrades and downtime, and privacy and security issues.

Participants that are acting as consumers of data will be required to provide at least one, but highly recommend two points of contact, known as **HIE Administrators** for CurrentCare Services. These administrators will be responsible for the maintenance of user profiles, including providing all necessary information to CurrentCare for adding users, deleting users, and assigning or changing user roles.

When a user's job status or role changes within an organization, if such change affects their access rights to the CurrentCare Services, HIE Administrators must promptly:

- **Change or remove the user's access/account**
- With each employee offboarding, HIE Admins should **assess if the user had access to MFT/SFTP** to upload or receive secure files. If that service needs to be terminated, the HIE Admin should promptly notify CurrentCare.

Organizations accessing CurrentCare Services through third- party EHRs, via SSO/SAML, will be responsible for terminating access through the EHR for the terminated user at the time of termination.

The HIE Administrators will also be responsible for attesting to the user identity verification and checking that users have completed all necessary policy training prior to obtaining access to the CurrentCare Services and for monitoring the general use and operations of the CurrentCare Services.

6.2 Implementation Support

CurrentCare and its HIE vendor(s) will make available the following implementation services (collectively, "Implementation Services") to the Participant:

- Establish environments (test and production) for secure transactions
- Conduct planning and decision sessions
- Jointly document transaction types
- Jointly document data conversion and mapping requirements

- Establish real-time notifications, if applicable
- Test and validate real-time notification, if applicable
- Establish batch transaction, if applicable
- Test and validate batch transactions, if applicable

7. Support

CurrentCare Support offers Participants end-user support and can be reached at Support@CurrentCareRI.org or 888-858-4815. CurrentCare Support uses a trouble ticket logging system that documents the severity and enables triage of the most severe problems. Depending on the nature of the issue, technical problems may be dealt with directly by CurrentCare Support or in certain situations may be raised to the attention of the applicable CurrentCare HIE vendor. For all reported and verified problems, CurrentCare will work to find a resolution in a timely manner and update Participants of actions taken as appropriate.

- CurrentCare Support provides support 8am-5pm EST Mon-Fri excluding holidays.
- The CurrentCare HIE vendor(s) provides support 24 hours a day, seven days a week, including weekends and some holidays.

8. Audit

All Participants are required to monitor, and audit access to and use of, their information technology systems in connection with CurrentCare Services and in accordance with their usual practices based on accepted health care industry standards and Applicable Law.

CurrentCare regularly reviews the usage of Participating User access of patient records and will enforce any misuse of a Participating User to include and up to termination of CurrentCare Services access. Notwithstanding, CurrentCare does not, and does not endeavor to, review each access by each Participant User. CurrentCare uses a privacy tool for additional monitoring of all user activities around protected health information access to ensure all provisioned accounts are being used appropriately and to protect protected health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of CurrentCare Services by Participant and Participant Users.

9. Report of Breach

Participant must notify CurrentCare's Privacy and/or Security Officer immediately in the event of any proven or suspected security incident in which Participant has reason to believe any unauthorized person may have had access to CurrentCare, or an unauthorized breach, access, use or disclosure occurred, including any and all available information that it has in its possession including:

(a) a description of what happened, including the date of the breach and the date of the discovery of the breach;

(b) a description of the types of data accessed through CurrentCare that were involved in the breach;

(c) a description of what Participant did to investigate the breach, protect against further breaches and mitigate harm; and (d) the identity of the person to contact for questions related to the breach.

In the event of a Breach of protected health information sent, received, found, or used via CurrentCare Services requiring notification to individuals under Applicable Law, the parties will handle the notification as set forth in the Agreements.

10. CurrentCare Advisory Committees

CurrentCare utilizes a committee structure that encourages community involvement and transparency in the process of the development and implementation of its policies.

These committees provide guidance and input to CurrentCare management on key decisions regarding CurrentCare Services. The Advisory Groups are intended to be broad-based to ensure that a breadth of interested stakeholders have the opportunity to participate and represent their constituencies.

Clinical Advisory Committee

Made up of representatives from clinicians from participating organizations.

Technical Advisory Committee

Includes technical subject matter experts from healthcare facilities in Rhode Island.

CurrentCare Community Advisory Committee

Made up of key community stakeholders who help provide patient-level and community-level input on CurrentCare activities.

11. Standards

CurrentCare aims to support CurrentCare Services in a standards-compliant manner and will use industry standard practices and generally accepted standards when possible and appropriate that are recognized by State, Federal, or industry authorities.

12. External HIE Participation

CurrentCare shares data with, and receives data from, External HIEs and National Networks (such as the eHealth Exchange) as defined by the CurrentCare Agreements. These External HIEs include, but may not be limited to, other state or local HIEs, including those managed by the Tech Vendor (CRISPSharedServices.org).

The following are permitted uses for data from the National Networks:

a) **Permitted Use**: Participant shall only transact message content for the permitted purpose of Treatment, as defined under HIPAA.

b) **Future Use**: Participant acknowledges that another participant entity may retain, use, and re-disclose message content in accordance with applicable law and its record retention policies once message content shared for a Treatment use case has been ingested into its EHR.