

Rhode Island Health Information Exchange

Approved

RI HIE Policy and Procedure

Subject: Role-based Permissions for the RI HIE	Related Policies: Patient Authorization for the RI HIE
Stakeholder Group: Steering Committee	Submission Date: March 27, 2008
Target Implementation Date: TBD	Date of Scheduled Review: TBD

BACKGROUND AND PURPOSE: The RI HIE will implement a range of policy and technical safeguards to protect the confidentiality of patient health information. System access parameters are defined to align with current organizational structures, roles and information access practices while supporting the need for active security controls and meaningful audit trails within the HIE. The purpose of this policy is to define a core set of user roles that encompass all anticipated user types and to define which rights (i.e., information access parameters, system functions) are permitted for each role.

BRIEF DEFINITION: Role-based Permissions (a.k.a., role-based authorization) is a security technique that enables or disables options for accessing functions and/or information in a given electronic system depending on the user's role. A defined set of roles are established for the HIE, encompassing a set of rights or permissions to indicate which system functions a user in that role may perform and what information users in that role may read, enter, change, update and/or delete through a computer terminal. As part of user registration with the HIE, the unique identifying information for each authorized user of the HIE will be associated with a role. When the user signs on to the HIE, a *user access profile* is invoked and the user's permissions related to system functions, patient records and content within those records are controlled accordingly.

Access privileges must be updated to reflect changes in user roles, employment or any other applicable user event. Appropriate security measures will be taken to minimize the possibility of unauthorized access to secure data by those who are no longer authorized to have access to that information.

RESPONSIBILITY:

The entity responsible for assuring policy compliance:

- Initial HIE development, testing and implementation: EDS under contract to RI Department of Health via RI HIE Security Administrator (an EDS-provided technical resource)
- Ongoing HIE operations: RI Department of Health until transfer of operations to RI RHIO, then RI RHIO via RI HIE Security Administrator (technical resource) and RI HIE Privacy/Security Officer (RHIO-provided resource).

POLICY

1. **User Roles and Permissions.** The RI HIE will maintain *user access permission profiles* to specify which system functions and protected health information (PHI) may be accessed by authorized users according to the specific role classification to which they are assigned. User access permission profiles are based upon two principles: First, that access to information must not be so restricted as to interfere with the quality or efficiency of patient care; and second, that access shall be sufficiently restricted to afford privacy and security to patients' information. The following System User Roles and Permissions will be implemented in user permission access profiles in the RI HIE:

RI HIE User Role	Role Description	System Permissions														
		Temporary Authorization (a.k.a., BTG)	Search / View demographic data in HIE	View / Print from HIE	View / Copy from HIE	Export from HIE	Set PT Viewing Authorization	Merge / unmerge Records	System Admin / Maintenance	Data Quality / Reporting	Create/Edit User Access Controls	Enroll / Update PT demographic data	Disenroll Patients	Submit Data to HIE		
Clerical / Admin / Enrollment	A designated non-clinical employee from the healthcare provider's facility and/or enrollment support personnel. * <u>view, copy and print permissions apply to demographic data only</u>		✓	✓*	✓*		✓							✓		
Licensed Non-independent Practitioner	Clinical support staff from the healthcare provider's facility, for example, nurses. <u>All permissions apply to demographic and clinical data.</u>		✓	✓	✓	✓										
Licensed Independent Practitioner (LIP)	All medical professionals responsible for patient care decision-making, including primary care providers, specialists, consultants, mid-level practitioners (midwives, nurse practitioners, etc.), among others as appropriate.	✓	✓	✓	✓	✓								✓		

RI HIE User Role	Role Description	System Permissions												
		Temporary Authorization (a.k.a., BTG)	Search / View demographic data in HIE	View / Print from HIE	View / Copy from HIE	Export from HIE	Set PT Viewing Authorization	Merge / unmerge Records	System Admin / Maintenance	Data Quality / Reporting	Create/Edit User Access Controls	Enroll / Update PT demographic data	Disenroll Patients	Submit Data to HIE
Data Submitting Partner	An entity contributing original source data to the RI HIE system.													✓
RI HIE Data Management Specialist	A person responsible for data quality assurance, reporting, evaluation and analysis functions for the HIE.		✓	✓	✓	✓		✓		✓		✓	✓	
RI HIE User Management (decentralized)	A designated person from participating healthcare organizations responsible for assigning and maintaining local personnel roles and access controls according to HIE/RHIO policies.													✓
Overall System Administration														
RI HIE Security Administrator (RI HIE SA)	A person responsible for managing user access to the RI HIE system, i.e., assigning/changing user ID, passwords, permissions and privileges.									✓			✓	✓
RI HIE System Administrator and technical support	A “master user” who performs RI HIE system administration and configuration tasks such as configuring data sources and installing, maintaining and troubleshooting all HIE infrastructure components.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

2. **Minimum Necessary Rule**-- Access profiles comply with the MINIMUM NECESSARY RULE pursuant to a Business Associate Agreement (“BAA”) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”) and are used to limit electronic access to PHI.
3. **User Awareness of System / Information Access by Role**--Participating entities will be responsible for specifying how job descriptions map to defined HIE User Roles. The HIE / RHIO is responsible for including access levels in training materials to assure that each user is aware of what system functions and information are permitted to be seen and used in their specific role/s. Users will also be made aware of access control policies, procedures and system audit practices. The user is responsible for adhering to the intended level of permission granted by user role, organizational affiliation and patient authorization and reporting any discrepancies to the HIE Security Administrator.
4. **Termination of Access**—If a user no longer requires system access, if user permissions change, or if system use audits demonstrate protracted inactivity or unauthorized activity in specific user accounts, modification or termination of access privileges will be processed in the HIE as soon as possible and coordinated with the appropriate entities. This provision also applies to termination of access to specific types of PHI and/or system functions when the status of any user no longer requires access to specific types of information.
5. **Review of Roles and Permissions Matrix**—The user roles and permission matrix used to implement user access permission profiles will be reviewed and revised periodically, upon request of a participating organization when a new role is created, when a role changes significantly, or when experience shows a need to make a modification.

REFERENCES:

- 45 CFR § 164.314(a)(1)(i) and 164.314(a)(2)(i) and 164.502(e)(i)
- RI HIE Patient Authorization Policy