

Greater New Orleans Health Information Exchange (GNOHIE)

USER ACCESS CONTROL POLICY

Approval Date: 5-22-2012

Effective Date: 6-15-2012

Scheduled Review Date: 6-1-2013

Goal: The *User Access Control* policy aims to ensure that the Greater New Orleans Health Information Exchange (GNOHIE) and Participating Organizations and Members comply with all applicable laws in allowing Users to view information, and the type of information available to view, on the MirthResults component or any other component of the GNOHIE, including Mirth Care and Mirth Analytics (“Mirth”). Establishing protocols related to Users access of the protected health information (PHI) is essential to build trust among members and remain in compliance with federal and state privacy laws.

Scope: This policy applies to GNOHIE and data stored within GNOHIE.

Purpose: The GNOHIE is responsible for controlling User access to PHI available through the GNOHIE. In particular this policy defines two things with respect to access to the Mirth system:

- What a User can DO within the Mirth system (Roles, Privileges)
- Which patients a User can SEE (Access Controls)

Definitions:

GNOHIE (Greater New Orleans Health Information Exchange) means the health information exchange components, integration and interface engine, clinical data repository, master patient index, data warehouse, chronic care management system as well as analytical tools and ancillary support software.

Access Control means what data a User can see with regard to the GNOHIE.

Site Administrator means a User that administers and grants access at a site level where Providers and other users may access the GNOHIE.

Audit Event means any *defined* event which triggers an audit that shows who has accessed GNOHIE, when it was accessed and what operations were performed.

Encounters means instances of when a patient presents in a GNOHIE site for medical care and such care is populated into GNOHIE.

Power User means a User with access to administrative functions related to clinical data, can view clinical data based on Provider/site constraints.

Provider means a Participating Organization or Member of the GNOHIE.

Site means the location where the User treats patients and where data may originate to populate the GNOHIE.

Source means the originator of a data source, e.g. a particular clinic or hospital.

User means an individual granted access by GNOHIE Administration to access the GNOHIE based on Provider/site constraints.

Policy:

To access data within the GNOHIE a User MUST be assigned both a privilege and a User Access Control. For example if a User cannot view the Encounters page because the User does not belong to a Role with that Privilege, the GNOHIE blocks access without bothering to check the User Access

Greater New Orleans Health Information Exchange (GNOHIE)

USER ACCESS CONTROL POLICY

Approval Date: 5-22-2012

Effective Date: 6-15-2012

Scheduled Review Date: 6-1-2013

Controls. If a User can view the Encounters page, and is trying to view an encounter for a Source and they have only been granted access to a different source, access is denied.

Privileges

A privilege defines a page a User can access or an action a User can perform. This restricts access like a traditional ACL (Access Control List). Privileges are defined as regular expressions that check against the URL or keywords defined by the GNOHIE. Multiple privileges may be defined in one entry by separating them with commas.

Roles

Privileges are grouped to Roles then Roles are assigned to Users.

The administrator Role has more privileges. The Administrator Role may have full access to view and modify all data in Mirth or other elements of the GNOHIE whereas; the general User Role only has access to view patient data.

User Access Controls

The Administrator configures User Access Controls per User.

Site

Every non-administrator User must be granted access to a site. This allows User to view patients within that site.

Sources

A User may be given access to all sources or only some sources within a site.

Providers

A User may be associated to one or more Providers. That User can then only view patients for those Providers. The patient/Provider relationship can be defined at the patient and Provider level (e.g., a Primary Care Provider) or through individual clinical items (such as a Provider being copied on a Lab Result).

Options to override consent and "break the glass"

The GNOHIE supports storing and tracking of patient consent. When a patient has opted out of the GNOHIE and GNOHIE receives messages pertaining to this patient, it will store but not display that information. Overriding consent or "breaking the glass" will allow the User access to this information.

Greater New Orleans Health Information Exchange (GNOHIE)

USER ACCESS CONTROL POLICY

Approval Date: 5-22-2012

Effective Date: 6-15-2012

Scheduled Review Date: 6-1-2013

When a User attempts to view the records of a patient who has opted out they are presented with a screen that allows them to select what Provider is authorizing this override, what role the User/Provider is acting in, and what reason the User has to break the glass.

Only very high level GNOHIE system administrators (HIE developers and security officers) may bypass the break the glass screen. Other Users are authorized to break the glass, but must fill out the override form. Some Users do not have permission to break the glass at all and are outright denied access to patient records.

When a User breaks the glass, an Audit Event is recorded along with the standard access events indicating that a User broke the glass and the reasons they gave. This auditing occurs anytime an opted-out patient record is accessed.

Granting permission to override consent

There are two privileges to support breaking the glass:

- **Consent Override Bypass** - Allows a User to bypass the override consent form. This means that a User is allowed access to all records and will not be presented with the override consent form. The access to an opted-out record will still be logged.
- **Consent Override Allow** - Allows a User to fill out the override consent form. Before viewing an opted-out record the User will be presented with the form and must complete it before being allowed to view the data. Access is logged.

By default the Administrator role has Consent Override Bypass and the Power User role has Consent Override Allow.

A role with neither of these permissions assigned is not allowed to override consent and will be redirected to a permission denied page if they do somehow select a patient who has opted out.

User Account Information

Account Id - the username for this account

Display Name - the Users displayed name, typically full name

Email - email address for the User

Password - Password complexity is defined by Configuration Options. It is typically a minimum of 7 characters and numbers.

Bad Login Attempts - A counter showing the number of failed logins. Set to 0 to reset.

Account Locked - Check or uncheck this to lock/unlock the account. Locked accounts cannot log in.

Each Participating Organization and Member shall have a procedure to timely delete a User's account information at such time when the User is no longer affiliated with that Participating Organization and/or Member.

Greater New Orleans Health Information Exchange (GNOHIE)

USER ACCESS CONTROL POLICY

Approval Date: 5-22-2012
Effective Date: 6-15-2012

Scheduled Review Date: 6-1-2013

Accessible Sites

While adding new Users, Accessible sites option is only visible for non-administrator roles. Sets the sites that a User can see when they log in. Non-administrator Users must have access to at least one site.

Accessible Providers

Accessible Providers are only visible for non-administrator roles. The Accessible Provider selected grants Users access to clinical data for a particular Provider. Non-administrator Users must have access to at least one Provider.

Associated Policies:

1. *Patient Consent*
2. *Breach Notification*
3. *Data Use, Retention and Disclosure*

I hereby certify that the foregoing Policy entitled *User Access Control* was approved by the Administrative Committee on May 22, 2012.

_____, Administrative Committee Chairman
Signature

Printed Name

Date