| POLICIES AND PROCEDURES |
| --- |
| **TOPIC:** User Authentication |
| **DOCUMENT NUMBER:** 400 |
| **EFFECTIVE DATE**: January 30, 2014 |

## I. BACKGROUND AND PURPOSE

The purpose of this policy is to describe the process of proving, confirming, and validating that an individual is who he or she claims to be when accessing the WVHIN's Health Information Exchange as an Authorized User. This process is known as authentication.

## II. POLICY

All Authorized Users must be authenticated prior to accessing Protected Health Information through the WVHIN. The establishment of a functional set of authentication procedures is essential to ensuring that Protected Health Information is not illegitimately accessed by an unauthorized individual.

It is anticipated that the following individuals may become an Authorized User:

- Patients (if registered for access to the Patient Portal that is offered as a WVHIN service)
- Workforce members of any Participating Organization
- Workforce members of the WVHIN
- Workforce members of the WVHIN's Business Associates

Before any of the above individuals may be granted access to the WVHIN, they must be properly designated as an Authorized User under the Policy and Procedures for User Authorization (*see* Policy and Procedure Document Number 300).

The WVHIN will use a combination of operational practices and technological solutions to authenticate any Authorized User. The WVHIN will require compound single-factor authentication, which will be known as an Authorized User's Authentication Information. This compound single-factor Authentication Information will be based upon at least 2 things that an Authorized User uniquely knows (e.g., username and password). An Authorized User will have to utilize both aspects of his or her Authentication Information in order to be authenticated by, and thereby granted access to, the WVHIN. Strict controls must be placed upon the use of this Authentication Information, which must not be shared with any other individual besides the Authorized User to whom they are assigned.

Should legal requirements ever impose the need for two-factor Authentication Information, the WVHIN will establish procedures to ensure compliance with such laws.

The status of an Authorized User can change. The WVHIN must rely upon its Participating Organizations and contractors to immediately update the WVHIN so that Authorized User status can be terminated or amended, as necessary. Similarly, the WVHIN must rely upon its Participating Organizations and Business Associates to educate and oversee their Workforce to ensure that this User Authentication Policy is consistently followed. Any and all violations must be reported to the WVHIN so that appropriate safeguards can be taken to eliminate or mitigate the possibility of access to the WVHIN by any unauthorized individual.

## III. PROCEDURES

A. Patient Procedures.

1. A Patient will only be able to access the WVHIN directly if he or she registers for access to the WVHIN's Patient Portal.

2. If a Patient chooses to register for access to the WVHIN's Patient Portal, he or she must do so through his or her cooperating Participating Organization.

3. If a Patient wants to register for access to the WVHIN's Patient Portal through his or her Participating Organization, and in the process become an Authorized User for the purpose of accessing the WVHIN's Patient Portal, the identity of the Patient must be verified and authenticated by the Participating Organization.

4. Once a Patient's identity has been verified and authenticated by the Participating Organization, the Patient will then complete the registration process to obtain direct access to the Patient Portal on the WVHIN, including the execution of a Patient Portal Agreement. This registration process may be accomplished with paper forms signed by the Patient manually, or with an electronic form signed by the Patient electronically.

5. Once registered, the Patient will be provided a unique username and permitted to select a password. The password must be considered a robust password.

6. A Patient must change his or her password periodically to ensure ongoing security. A Patient will be reminded of this change to his or her password automatically by the WVHIN.

7. A Patient must complete the compound single-factor authentication process each time he or she accesses the WVHIN's Patient Portal. The WVHIN may establish a protocol to lock out a Patient from the Patient Portal if the Patient demonstrates a repeated failure to log-in properly. This lock out will be terminated only after the Patient's identity is verified and his or her password is reset by the WVHIN. A Patient is responsible for maintaining the privacy and security of his or her Authentication Information.

8. A Patient must immediately report any violation of this User Authentication Policy, the loss or misuse of his or her Authentication Information, or any other suspicious activity involving an unauthorized individual, to the WVHIN. If necessary to prevent imminent harm, the WVHIN will lock out the Patient in question from the Patient Portal. This lock-out will be terminated after the identity of the Patient is verified, and his or her password is reset. For purposes of this Policy and Procedure, the term "imminent harm" means harm to the Patient or the Health Information Exchange (for example, failure to cooperate, unauthorized access to the Health Information Exchange, including, but not limited to, malware or bot access to the Health Information Exchange), and the term "immediately" means within the same business day.

B. Participating Organization Procedures.

1. A Participating Organization must verify and authenticate the identity of any Patient who is seeking to register for access to the Patient Portal on the WVHIN. If the Participating Organization does not have personal knowledge of the Patient's identity, at least 1 valid form of photo identification must first be reviewed by the Participating Organization. Absent either personal knowledge or at least 1 valid form of photo identification, a Patient cannot register for access to the WVHIN's Patient Portal.

2. Before a Participating Organization may designate Authorized Users, and permit the development of Authentication Information on behalf of its Authorized Users, it must first execute a Participating Organization Agreement.

3. After executing a Participating Organization Agreement, the Participating Organization must properly designate a list of its Authorized Users from its Workforce in accordance with the Policy and Procedures for User Authorization (*see* Policy and Procedure Document Number 300).

4. Once an individual has been designated as an Authorized User by a Participating Organization, the Participating Organization's Site Administrator must ensure that each Authorized User establishes Authentication Information sufficient to allow the Authorized User to access the Health Information Exchange.

5. Once designated as an Authorized User, the Authorized User will be provided a unique username and permitted to select a password. The password must be considered a robust password.

6. An Authorized User must change his or her password periodically to ensure ongoing security. An Authorized User will be reminded of this change to his or her password automatically by the WVHIN.

7. An Authorized User must complete the compound single-factor authentication process each time he or she accesses the WVHIN. The WVHIN may establish a protocol to lock out an Authorized User from the Health Information Exchange if he or she demonstrates a

repeated failure to log-in properly. This lock out will be terminated only after the Authorized User's identity is verified and his or her password is reset.

8. An Authorized User cannot share his or her Authentication Information with any other individual.

9. A Site Administrator or Authorized User must immediately report any violation of this User Authentication Policy, a loss or misuse of any Authorized User's Authentication Information, or other suspicious activity involving any unauthorized individual, to the WVHIN. If necessary to prevent imminent harm, the Participating Organization's Site Administrator will lock out the Authorized User in question from the WVHIN. This lock out will be terminated after the identity of the Authorized User is verified, and his or her password is reset. For purposes of this Policy and Procedure, the term "immediately" means within the same business day.

10. A Participating Organization is responsible for keeping its list of Authorized Users up-to-date and current. This means that changes in employment as well as other changes to the status of the Workforce affecting an Authorized User of a Participating Organization must be communicated immediately to the WVHIN by the Site Administrator. Contemporaneous with such report, the Participating Organization's Site Administrator will lock out the former Authorized User in question from the WVHIN.

11. A Participating Organization's Site Administrator must immediately and electronically amend or terminate an Authorized User's status if he or she determines that an Authorized User's status has changed, or an Authorized User no longer has a need to access the WVHIN on behalf of the Participating Organization.

12. A Participating Organization and its Site Administrator will be wholly responsible for maintaining an appropriate and up-to-date list of its Authorized Users.

C. <u>WVHIN Procedures</u>.

1. The WVHIN must properly designate a list of Authorized Users from its Workforce in accordance with the Policy and Procedures for User Authorization (*see* Policy and Procedure Document Number 300).

2. In addition, the WVHIN must require any of its Business Associates and Participating Organizations to properly designate a list of Authorized Users from their respective Workforces in accordance with the Policy and Procedures for User Authorization (*see* Policy and Procedure Document Number 300).

3. Once designated as an Authorized User, the Authorized User will be provided a unique username and permitted to select a password. This password must be considered a robust password.

4. An Authorized User must change his or her password periodically to ensure ongoing security. An Authorized User will be reminded of this change to his or her password automatically by the WVHIN.

5. The WVHIN will maintain an encrypted database of all usernames and passwords that have been utilized by Authorized Users. The WVHIN must ensure that all usernames are unique to a single Authorized User.

6 The WVHIN will deny access to its Health Information Exchange to any Authorized User who does not complete the compound single-factor authentication process. The WVHIN may establish a protocol to lock out an Authorized User from the Health Information Exchange if he or she demonstrates a repeated failure to log-in properly. This lock out will be terminated only after the Authorized User's identity is verified and his or her password is reset.

7. Should legal requirements ever impose the need for two-factor Authentication Information, the WVHIN will establish procedures to ensure compliance with such laws.

8. The WVHIN will immediately lock out any of its Authorized Users or its Business Associates' Authorized Users who are reported to have violated this Policy, who lose or misuse their Authentication Information, or who are the victims of suspicious activity involving any unauthorized individual. This lock out will be terminated only after the identity of an Authorized User has been verified, and his or her password reset.

9. The WVHIN will maintain an up-to-date record of all Authorized Users who may access the WVHIN based upon information provided by its Business Associates and Participating Organizations.

10. The WVHIN reserves the right to terminate any individual's status as an Authorized User for good cause, including but not limited to, any fraudulent activity or other activity that constitutes a repeated and ongoing violation or abuse of this Policy.

11. The WVHIN may automatically lock out an Authorized User after a significant period of inactivity [after a designated period of time] if he or she has not accessed the WVHIN at any time during the prior 60 days. This lock out will be terminated only after the identity of an Authorized User has been verified, his or her password reset, or other appropriate mitigation measures have been taken.