USE

**AM007 Manage Password  
Use Case**

**Colorado Health Benefit Exchange (COHBE)**

**Version 1.0**

**November 15, 2012**

REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Modified By | Description |
| 0.1 | 10/23/2012 | Kelly J. Wiley | Draft for Discovery Review |
| 0.2 | 10/31/2012 | Diane Dunn | Updated from Discovery session |
| 0.3 | 11/06/2012 | Diane Dunn | Updated from Elaboration session |
| 0.4 | 11/09/2012 | Diane Dunn | Updates from the Verification Session |
| 1.0 | 11/15/2012 | Diane Dunn | COHBE Approved |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

TABLE OF CONTENTS

[1 Use Case: AM007 – Manage Password 6](#_Toc340578013)

[1.1 Goal 6](#_Toc340578014)

[1.2 Brief Description 6](#_Toc340578015)

[1.3 Requirements Traceability 6](#_Toc340578016)

[1.4 Primary Actor 7](#_Toc340578017)

[1.4.1 Exchange 7](#_Toc340578018)

[1.4.2 User 7](#_Toc340578019)

[1.5 Secondary Actor 7](#_Toc340578020)

[1.5.1 Service Representative 7](#_Toc340578021)

[1.6 Pre-Conditions 7](#_Toc340578022)

[1.7 Successful Post-Conditions 8](#_Toc340578023)

[1.8 Triggers 8](#_Toc340578024)

[1.9 Assumptions 8](#_Toc340578025)

[2 Flow of Events 8](#_Toc340578026)

[2.1 Basic (Main) Flow – Manage Password 9](#_Toc340578027)

[2.1.1 Created by Third Party? 9](#_Toc340578028)

[2.1.2 Is User Fully On-Boarded? 10](#_Toc340578029)

[2.1.3 Will Password Expire Soon? 10](#_Toc340578030)

[2.1.4 Voluntary Change of Password? 10](#_Toc340578031)

[2.1.5 Can User Manage the Lockout (SOFT LOCK)? 10](#_Toc340578032)

[2.1.6 Must Service Representative Manage Lockout (HARD LOCK)? 11](#_Toc340578033)

[2.1.7 Update Account 11](#_Toc340578034)

[3 Alternate Flows 12](#_Toc340578035)

[3.1 Generate Notice with Temporary Password 12](#_Toc340578036)

[3.1.1 Generate Notice with Temporary Password 12](#_Toc340578037)

[3.2 Know Temporary Password? 12](#_Toc340578038)

[3.2.1 Know Temporary Password? 12](#_Toc340578039)

[3.2.2 Service Representative Sets Temporary Password 12](#_Toc340578040)

[3.2.3 Give Temporary Password Verbally? 12](#_Toc340578041)

[3.2.4 Generate Notice with Temporary Password 13](#_Toc340578042)

[3.3 Password Expiration Warning 13](#_Toc340578043)

[3.3.1 Pop-up Warning Notice of Expiration 13](#_Toc340578044)

[3.4 Needs Service Representative Assistance 13](#_Toc340578045)

[3.4.1 Service Representative Sets Temporary Password 13](#_Toc340578046)

[3.4.2 Give Temporary Password Verbally? 13](#_Toc340578047)

[3.4.3 Generate Notice with Temporary Password 14](#_Toc340578048)

[3.4.4 Set New Password 14](#_Toc340578049)

[4 Exception Flows 14](#_Toc340578050)

[4.1 User Abandons Manage Password 14](#_Toc340578051)

[5 Specifications 14](#_Toc340578052)

[5.1 Business Rules 14](#_Toc340578053)

[5.1.1 Temporary Password Rules 14](#_Toc340578054)

[5.1.2 Password Expiration Rules 15](#_Toc340578055)

[5.2 Process Rules 16](#_Toc340578056)

[5.2.1 Third Party User 16](#_Toc340578057)

[5.3 Workflow 16](#_Toc340578058)

[5.4 UI Screen Details 16](#_Toc340578059)

[5.4.1 UI Flow Considerations 16](#_Toc340578060)

[5.4.2 My Account 16](#_Toc340578061)

[5.5 Communications 16](#_Toc340578062)

[5.5.1 Imaging Requirements 16](#_Toc340578063)

[5.5.2 Form Requirements 17](#_Toc340578064)

[5.5.3 Notice Requirements 17](#_Toc340578065)

[5.5.4 Other Communication Requirements 17](#_Toc340578066)

[5.6 Interfaces 17](#_Toc340578067)

[5.7 Reporting 17](#_Toc340578068)

[5.7.1 User Experience 17](#_Toc340578069)

[5.7.2 Business Activity 17](#_Toc340578070)

[5.7.3 Workflow 18](#_Toc340578071)

[5.7.4 Community and Public Health 18](#_Toc340578072)

[5.8 User Security 18](#_Toc340578073)

[5.8.1 Password Security Properties 18](#_Toc340578074)

[5.8.2 Transition States 18](#_Toc340578075)

[5.9 Activity Log and Audit Trail 18](#_Toc340578076)

[5.9.1 Activity Log 18](#_Toc340578077)

[5.9.2 Audit Trail 19](#_Toc340578078)

[5.10 Data Elements 20](#_Toc340578079)

[6 Future Release Notes 21](#_Toc340578080)

[7 Appendix A - Glossary 21](#_Toc340578081)

# Use Case: AM007 – Manage Password

## Goal

The goal of this Use Case is to manage all aspects of the Password process in the Exchange for any and all Actors that will be using The Exchange in any way.

This Use Case completes successfully when an actor is able to log in to the Exchange with the proper password and use the Exchange.

## Brief Description

Any user of The Exchange will need to log in with a Log In ID and Password.

## Requirements Traceability

The following requirements are covered within this Use Case:

* AM180 – The System shall have the capability to require a password to be changed after a defined period of time based on role.
* AM181 – The System shall have the capability to enable the customer to automatically reset their password using a set of security-related questions.
* AM190 – The System shall have the capability to enable authorized personnel to force a customer to change their password upon next login.
* AM200 – The System shall have the ability to send a System generated email notification of password change events and expiration warnings in compliance with COHBE password and security policy requirements.
* AM230 – The System shall have the ability to suspend access after a specific number of unsuccessful log-in attempts.
* AM240 – The System shall have the administrative controls to enable an administrator to disable online access for a user. \*\*\* This Requirement will also be included to the AM016-Manage Login Use Case.

## Primary Actor

### Exchange

The Exchange will be the primary actor, as it will evaluate whether an account has been created.

### User

A user may be an individual, an employee, an employer, a broker, a navigator entity, or a navigator.

## Secondary Actor

### Service Representative

The Service Representative will be a secondary actor, helping a user in managing their password.

## Pre-Conditions

* The Create Individual Account Use Case must be executed prior to the Individual or employee managing their password.
* The Create Employer Account Use Case must be executed prior to the Employer managing their password.
* The Create Navigator Entity and Navigator Account must be executed prior to the Navigator Entity or Navigator managing their password.
* The Create Broker Account Use Case must be executed prior to the Broker managing their password.
* The Create Back Office/Service Representative/COHBE/DOI Account Use Case must be executed prior to the Actor managing their password.
* The Create Carrier Account Use Case must be executed prior to the Carrier managing their password.
* The user remembers their log in ID.
* Data elements to be populated and verified prior to this Use Case include:
  + Log in ID
  + Name
  + Email (if provided)

## Successful Post-Conditions

* The user’s account has been updated with password and security questions as appropriate.
* Data elements listed as required in section 5.10 are populated.

## Triggers

There are several triggers for having to manage a password:

* Expired Password
* Forgotten Password
* Too many failed attempts to login
* Disabled online access for a user
* User receive temporary password via notice
* User wants to change Password

## Assumptions

* User remembers their Log In ID. If the user has forgotten their Log In ID, Manage Log In ID Use Case will address that situation.
* Users may have more than one account on the Exchange across various portals (individual, SHOP, Broker, Navigator Entity).
* Users may have more than one account in a portal and it may be that not all of those are legitimate. COHBE accepts this risk.

# Flow of Events

The Business Process Activity diagram below shows the COHBE processes for the Manage Password Use Case. The steps numbered on the diagram below have detailed explanations in the sections that follow.



## Basic (Main) Flow – Manage Password

The main flow is one that contains several branches. The Exchange will evaluate if the account was created by a third party. If not, the user can then choose to voluntarily change their password, can reset their password due to a soft lock out (able to manage for themselves), contact a service representative if there is a hard lock out (requires assistance) or set their security questions and answers.

### Created by Third Party?

Was the account created by the user or a third party? If the user created the account for themselves, the flow proceeds to 2.1.2 Is User Fully On-boarded? If the account was created by a third party, such as a broker for an employer or a navigator entity for a navigator, the flow goes to the alternate flow at step 3.1.1 Generate Notice with Temporary Password.

### Is User Fully On-Boarded?

A user is fully on-boarded if they have an account created with a password they set themselves and the security questions and answers set. If the user has completed the password and security questions they can proceed to step 2.1.3 Will Password Expire Soon? If the user has not completed their on-boarding, they go to alternate step 3.2.1 Know Temporary Password?

### Will Password Expire Soon?

The system will evaluate if the password will expire soon. “Soon” is defined for each user role in the business/process rules of Section 5.1. If it will expire soon, the process goes to the alternate flow at step 3.3.1 Pop-Up Warning Notice of Expiration. If the password is not expiring the process continues on to step 2.1.4 Voluntary Change of Password?

### Voluntary Change of Password?

A user may want to change their password voluntarily because the password is about to expire or because they just want to change it. This is not due to a lock out condition (such as too many attempts). If they want to change, the process goes to step 2.1.4.1 Enter Old Password, Reset to New Password.

#### Enter Old Password, Reset to New Password

The user should enter their old password, which may be the temporary one, and then set a new password. When done, the process goes to step 2.1.4.2 Set Security Questions and Answers for the First Time?

#### Set Security Questions and Answers for the First Time?

The user may choose to update the Security Questions and Answers. If they choose to do so, the process goes to step 2.1.4.3 Select Questions, Give Answers. If not, the flow goes 2.1.7 Update Account.

#### Select Questions, Give Answers

The user can chooses security questions and will need to provide answers to those questions. All three question and answer sets must be completed. When done, the user clicks Save and the flow goes to 2.1.7 Update Account.

### Can User Manage the Lockout (SOFT LOCK)?

A soft lock is when the system locks a user out of their account and they have forgotten their password, their password is expired and they don’t remember it, etc. The soft lock status is role-based and indicates that a user can reset the password themselves by answering the security questions. If the user can manage their own password reset, the flow goes to 2.1.5.1 Remember Security Answers? If the user cannot manage their own password reset, the flow goes to 2.1.6 Must Service Representative Manage Lockout (HARD LOCK)?

#### Remember Security Answers?

The user may or may not remember their security answers or they may type in the answers wrong (case sensitivity, wrong punctuation, etc.). If the user remembers the answers, the flow goes to 2.1.5.2 Answer Security Questions to Reset. If the user does not remember their security answers, they enter the alternate flow at 3.4.1 Service Representative Sets Temporary Password.

#### Answer Security Questions to Reset

The user enters the security answers (correctly) in this step to unlock their account. When done, the flow goes to 2.1.5.3 Set New Password.

#### Set New Password

The user can now reset their password by entering a new value. When done the flow proceeds to step 2.1.7 Update Account.

### Must Service Representative Manage Lockout (HARD LOCK)?

A hard lock is very similar to a soft lock but is set when the user role is one with access to more sensitive data. The users may be COHBE staff, Navigator Entities, or Back Office Staff. (Service Representatives will have their accounts reset by another authorized user who is empowered to handle their level of security.) The hard lock status indicates that a user must call a Service Representative to reset their account. If the user is in this situation, the flow goes to the alternate step at 3.4.1 Service Rep Sets Temporary Password. If the user is not in a hard-lock status, the flow continues on to 2.1.7.2 Next Steps.

### Update Account

The Exchange saves the updates to the account and goes to step 2.1.7.1 Send Confirmation.

#### Send Confirmation

The Exchange will send a confirmation email to the user that the account was updated. At this point, the flow goes to 2.1.7.2 Next Steps.

#### Next Steps

The user may go to any number of places on the application (without logging out and back in), including:

* Manage Account Information
* Manage Employee Roster
* Maintain Book of Business, etc.

# Alternate Flows

## Generate Notice with Temporary Password

If the account is created by a third party (employer, broker, navigator entity, service representative), the system must generate a temporary password.

### Generate Notice with Temporary Password

The Exchange, upon evaluating the account was created by a third party, will set a temporary password. A notice is sent using the preferred communication (email or mail). The temporary password is included in the notice. Once sent, the flow then reenters the main flow at step 2.1.2 Is User Fully On-Boarded?

## Know Temporary Password?

If the User is not fully on-boarded (i.e., does not have a password and security questions/answers), the system will ask for the password to be reset from the temporary password.

### Know Temporary Password?

If the user has their temporary password from the notice, the user can reenter the main flow at step 2.1.4.1 Enter Old Password, Reset to New Password. If the user cannot use their temporary password (lost notice, did not act before it expired), the system will instruct them to call the Service Center to speak to a representative in step 3.2.2.

### Service Representative Sets Temporary Password

Once the Service Representative has been contacted by the user, the Service Representative can initiate a password reset by instructing the system to generate a temporary password. The user will be given a choice of how to receive the temporary password in step 3.2.3 Give Temporary Password Verbally?

### Give Temporary Password Verbally?

The user will be given the opportunity to hear the password while on the phone with the Service Representative. This allows the user to try the temporary password while still on the call with the Service Rep (and he/she can prompt the user as needed). If the user chooses to hear it verbally, the flow re-enters the main flow at step 2.1.4.1 Enter Old Password, Reset to New Password. If they would rather receive the password via their preferred communication (mail or email), the flow goes to step 3.2.4 Generate Notice with Temporary Password.

### Generate Notice with Temporary Password

The Exchange will generate a notice with the temporary password using the preferred communication method. Once sent, the flow then reenters the main flow at step 2.1.4.1. Enter Old Password, Reset to New Password.

## Password Expiration Warning

When the password is set to expire soon, the system will give a pop-up warning notice. The expiration times as well as the notice lead time are role based and discussed in Section 5.1.

### Pop-up Warning Notice of Expiration

The system will show a pop-up warning of the password expiration when the user signs in to the Exchange. Once displayed, the flow reenters the main flow at step 2.1.4 Voluntary Change of Password?

## Needs Service Representative Assistance

The user may need the assistance of the Service Representative. It may be because they don’t remember their security answers or it may be because their user role requires a hard lock that must be unlocked by a Service Representative.

### Service Representative Sets Temporary Password

Once the Service Representative has been contacted by the user, the Service Representative can initiate a password reset. The user will be given a choice of how to receive the temporary password in step 3.4.2 Give Temporary Password Verbally?

### Give Temporary Password Verbally?

The user will be given the opportunity to hear the password while on the phone with the Service Representative. This allows the user to try the temporary password while still on the call with the Service Rep (and he/she can prompt the user as needed). If the user chooses to hear it verbally, the flow goes to 3.4.4 Set New Password. If they would rather receive the password via their preferred communication (mail or email), the flow goes to step 3.2.3 Generate Notice with Temporary Password.

### Generate Notice with Temporary Password

The Exchange will generate a notice with the temporary password using the preferred communication method. Once sent, the flow then goes to 3.4.4 Set New Password.

### Set New Password

The notice will have the temporary password in it which allows the user to set a new password. When done, the flow reenters the main flow at step 2.1.7 Update Account.

# Exception Flows

## User Abandons Manage Password

The user may choose to exit the Use Case at any time without setting their password or security questions. If the user is locked out from the application, no further work can be done. If the user is signed in and not locked, they may proceed to other areas of the website. In order to set the password and/or security questions and answers, the use case will need to be restarted.

# Specifications

## Business Rules

### Temporary Password Rules

The system will generate the temporary password according to the compliance rules. The actual structure will be determined during the detail design.

### Password Expiration Rules

This is a draft of the Security Matrix; it is intended to be a placeholder representing possible paramaters to be used. The Security Horizontal deliverable will be the official record of parameters.

Passwords will expire after a time. The rules for expirations will be:

| User Role | Password Expiration Time (set based on roles) | Warning Lead for Expiration | Method of Sending Warning Notice | Temporary Password Expiration Time (Same as regular) | Grace Log Ins (after password has expired) | Soft Lock | Hard Lock |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Individuals and Employees | 12 months | 30 days | On Screen Warning | 12 months | 5 Log Ins | X |  |
| Employers | 12 months | 30 days | On Screen Warning | 12 months | 5 Log Ins | X |  |
| Brokers | 90 days | 15 days | On Screen Warning | 90 days | 5 Log Ins | X |  |
| Navigator Entities | 90 days | 15 days | On Screen Warning | 90 days | 5 Log Ins |  | X |
| Navigators | 90 days | 15 days | On Screen Warning | 90 days | 5 Log Ins | X |  |
| Carriers | 90 days | 15 days | On Screen Warning | 90 days | 5 Log Ins |  | X |
| Service Representatives | 30 days | 7 days | On Screen Warning | 30 days | 1 log in |  | X |
| Back Office Staff | 30 days | 7 days | On Screen Warning | 3 days | 1 log in |  | X |
| CGI Maintenance Staff | 30 days | 7 days | On Screen Warning | 3 days | 1 log in |  | X |
| COHBE Staff | 30 days | 7 days | On Screen Warning | 3 days | 1 log in |  | X |

See 5.5.3 for notices around password expirations. These rules will be refined in Detail Design.

## Process Rules

### Third Party User

A Third Party User is determined by the log in ID and what type of account it is compared to the user’s account. A third party is:

* An employer for an employee
* A broker for an individual, an employee, or an employer
* A Service Representative for any other actor.

Note that a Navigator should never be a Third Party because they are not to create accounts for anyone.

## Workflow

There are no workflow needs for the Manage Password Use Case. Service Representatives will have workflows determined through the Service Center Statement of Work.

## UI Screen Details

### UI Flow Considerations

The screens will be in the My Account area of the application. The screens are called from the various Account Management (AM) Manage…. Information Use Cases.

### My Account

For each type of actor, there are My Account screens associated with the account. In each of those, there are screens with the Password and Security Questions and Answer fields. No new screens are needed. It is recommended that the Password reset and Security Questions and Answers be presented on a single screen.

## Communications

### Imaging Requirements

No documents or files are expected in this Use Case and therefore there are no Imaging Requirements for the Manage Password Use Case.

### Form Requirements

There are no form requirements for the Manage Password Use Case.

### Notice Requirements

#### Temporary Password Notices

Notices will be generated according to roles (see Section 5.1.1) and communication preferences on file. The notice will include the temporary password.

#### Notice of Account Update

Notices (based on communication preferences) will be sent after every update to an account. This confirmation notice will advise the user that an update was made and to contact the Service Center if they did not make the change.

### Other Communication Requirements

#### Warning Notice of Password Expiration

Warnings will be displayed on-screen to all users based on their roles and communication preferences. The expiration warning time will vary by role.

## Interfaces

There are no interfaces for the Manage Password Use Case.

## Reporting

### User Experience

* Page abandonment rates

### Business Activity

* Number of accounts updated (total)
* Service Representative Resets by User Type
* Number of self-service resets
* Top ten users requesting temporary passwords
* Frequency of temporary password delivery methods

### Workflow

### Community and Public Health

* Report on number of Users with Active Accounts each month, by type of account.

## User Security

The User Security details listed in this Use Case are not intended to be a full reference of User Security requirements for the project. This section houses User Security requirements that are specific to this Use Case.

### Password Security Properties

Password security properties will be addressed by separate deliverable. It is part of the Security Horizontal review.

### Transition States

The transition states here are representative and not a complete list. Accounts may be:

* Active – No problems with the account
* Soft Locked – role based, allows a user to reset their password using the security questions and answers
* Hard Locked—role based, requires a Service Representative or other authorized user to generate a temporary password
* Temporary Security – lacks a password as well as security questions and answers
* Temporary Password – security questions and answers exist, but the password is a system-generated temporary password
* Inactive – deceased, decertified, or otherwise no longer active.

## Activity Log and Audit Trail

The Activity Log and Audit Trail details listed in this Use Case are not intended to be a full reference of Activity Log and Audit Trail requirements for the project. This section houses Activity Log and Audit Trail requirements that are specific to this Use Case.

### Activity Log

* Account modification that requires Service Center or Back Office assistance.
  + On-line
  + Phone

### Audit Trail

* Who modified the account, by type of account. Categorize by broker, entity, navigator, service representative, back office staff
* Who accessed the account or modified the account outside of the broker, entity, or navigator ID (owner of the account)

## Data Elements

| Process Step Reference  **\*Required Field** | Field Name  **\*Required Field** | Required Field? | Action Taken | Actor Performing Action | Format, if known |
| --- | --- | --- | --- | --- | --- |
| 2.1.4.1  2.1.5.3  3.4.4 | Password | * Required | * Reenter | * User | * Follows Password Security |
| 3.1.1  3.2.4  3.4.3 | Password | * Required | * Temporary Password Generated | * System | * Follows standard for temporary passwords |
| 2.1.4.2  2.1.4.3 | Security Questions and Answers (1, 2, 3) | * Required | * Entered | * User | * Alphanumeric, allow embedded spaces, special characters |
| None | Security Questions and Answers (1, 2, 3) | * Required | * Modification | * System Administrator only | * Once entered, questions and answers can only be modified by exception * Alphanumeric, allow embedded spaces, special characters |

# Future Release Notes

Set temporary passwords to expire at different times based on the method of delivery (verbal, email, mail) rather than just by role.

Allow for modifications by users of Security Questions and Answers after they are set.

# Appendix A - Glossary

| Term | Definition |
| --- | --- |
| Account | An “Account” is the means by which a user can access a computer system |
| Activity Log | An “Activity Log” is a chronological record of every action taken by each user, and by the System on behalf of each user.  The activity log includes actions and events pertaining to transactions, workflow, security (including SIEM), Alerts, Notifications, Approvals and interactions between the user and the System such as submissions of forms, data and documents. |
| Audit Trail | An “Audit Trail” is a subset of records in the Activity Log that are selected and correlated by criteria provided by the auditor or requesting authority. |
| Brokers | “Brokers” are persons authorized to assist Employers and or Individuals in their activities to shop for insurance through the Exchanges. |
| Carriers | “Carriers” are providers of insurance who will sell Qualified Health Plans (QHPs) in the Exchange. Occasionally, the term Health Plans is used to mean Carriers. Where it is not clear if the term Health Plan means an offering of a Carrier or the Carrier itself, the context should be used to help clarify meaning. Carriers may also be referred to as “Issuers”. |
| COHBE | Colorado Health Benefit Exchange, “COHBE” is used interchangeably with “Exchange” throughout the documents. |
| Customer | “Customers” or “Consumers” may be used interchangeably and are terms meant to define individuals or small employers or employees of small employers learning about opportunities to purchase, shopping to purchase, purchasing insurance through the Exchange, or modifying insurance purchased through the Exchange. References to Customers include, as appropriate, dependents of Customers, employees and dependents of employees and others covered by insurance purchased by Customers through the Exchange. |
| Employer | An “Employer” is a company or small business who participates in the Exchange to offer insurance and/or premium assistance to its Employee(s) or its Employee(s) and their dependents. |
| Exchange | During the implementation phase, the terms “Exchange” or “Exchanges” are meant to include technology, services, business processes, people, and other resources required to implement, operate and/or maintain the requirements or functions needed to support the ability for consumers to shop for and purchase health insurance. Specifically related to interpretation of a requirement, the term “Exchange” implies that the implementation of a requirement is not strictly limited to a technology solution.   * Individually, the term “Exchange” refers to each Exchange or both Exchanges as appropriate in the context. * The Exchange is NOT a state agency but a standalone non-profit entity. It will serve as an aggregator of individual policies sold by private insurers and underwritten using the new federal and state underwriting and rating rules. * The Small Business Health Options Program (SHOP) Exchange will support the specific needs of small employers. * For context, the Exchanges will act much like an “Expedia or Orbitz for Health Insurance” system. They will allow individuals and small firms to obtain information, compare and purchase private health insurance plans. The Exchanges will also be the entities that will evaluate whether or not a particular insurance policy meets the criteria set out by the new federal rules for policies offered to individuals and small employers. |
| Service Representatives | Service Representative (ServRep or SR): A COHBE representative who assists Participants, Customers, and/or Users in using the Exchange and/or the System. NOTE: CSR is used to mean Cost Sharing Reductions and shall not be used to mean ‘customer service representative’. |
| SHOP | Small Business Health Options Program |
| System | The “System” means all of the software, configurations, data, processes, and equipment used to provide the Exchanges and the System is also referred to as the “solution.” During the implementation phase, “System” is taken to mean the technology component of the Exchange. |
| Users | “Users” are users of the Exchange authorized by COHBE and may include operators, administrators, customers, brokers, navigators, etc., who interact with the System. Users may be internal or external to COHBE. |
| Hard Lock | Role based, requires a Service Representative to generate a temporary password. |
| Soft Lock | Role based, allows a user to reset their password using the security questions and answers. |
| Temporary Security | Lacks a password as well as security questions and answers |
| Temporary Password | Security questions and answers exist, but the password is a temporary temporary password |