COI·SMART

**COI-SMART Limited
Edition (LE)
Administrator Guide - Beta Version**

February 15, 2016

TABLE OF CONTENTS

1. Introduction

1.1   About HCCS

The mission of HCCS, A HealthStream (NASDAQ: HSTM) Company, is to help hospitals and healthcare institutions survive and thrive, and to improve the quality of patient care. Our method for accomplishing that mission is to provide hospitals and healthcare institutions with interactive and engaging on-line staff learning and competency solutions, and tools to assist in the management of difficult compliance problems. These solutions enhance job performance, improve patient outcomes and promote compliance with ethical, legal and accreditation guidelines. In this way, healthcare institutions can focus on their core mission of easing discomfort, healing, and saving lives.

HCCS is the leading provider of effective online compliance and competency training courses, learning management systems and database management tools to healthcare facilities.

You can reach HCCS at our website, www.hccs.com, the COI-SMART website at www.coi-smart.com or by email at support@hccs.com. Our corporate offices can be reached at 516-478-4100.

1.2   COI-SMART Limited Edition (LE)

COI-SMART is a well-established web-based tool for the management of conflicts of interest. Its comprehensive feature set has helped many hospitals, academic medical centers, and health systems handle complex, high volume disclosure processes, managing conflicts of interest related to research, the IRS and fiduciary responsibilities. **COI-SMART** has the largest installed base of any COI management tool, and has been rolled out in more than 500 locations.

The Challenge: Many smaller and less complex organizations have sought to automate their own paper-based COI disclosure processes, but have not been able to support the expense associated with a full featured COI management system. In many places, institutions manage conflicts of interest for a small number of influential board members and physicians, and would like to professionalize a process which has always been manual and labor intensive. Now, **COI-SMART Limited Edition** (LE) brings many of the features of COI-SMART to smaller, or less complex, organizations at an affordable cost.

COI-SMART LE is designed to accommodate three basic categories of users:

- "Respondents" are users who access the system to complete disclosure questionnaires.
- "Reviewers" are users who are authorized to review and take action on the questionnaires of respondents. (A Reviewer is often also a Respondent).

- "Administrators" are users with limited administrative rights to the system. They can modify user profiles, run reports and otherwise manage the COI-SMART LE system. (An Administrator is often a Respondent and can also be a Reviewer).

The COI-SMART LE system can provide custom questionnaire content based on a respondent's role (or roles) within the organization. Reviewers will have access to the disclosures of all individuals within the system.

The COI-SMART LE program is designed to be user-friendly, particularly for respondents who come into contact with the program infrequently. Users are able to access their questionnaire from, a web browser that is connected to the Internet, to provide initial disclosures and to revise information going forward. See appendix B for supported web browsers.

A user (respondent) initially accesses the system when they receive an email from the COI-SMART LE system. That email will include a link which will bring them to a login screen. The first time they access the system they will be asked to set a unique password. They will then be brought to a default announcement screen which will introduce them to the COI-SMART LE system. Reminder emails can be automatically sent to remind respondents to submit questionnaires.

When answering the questionnaire, respondents proceed through a series of intuitive and easy-to-navigate screens to answer questions. When they have completed every required question, they will be asked if they want to submit their questionnaire.

COI-SMART LE includes a module that allows an authorized individual to manually enter questionnaire responses on behalf of someone else, so that information originally provided on paper can then be analyzed and reported electronically. If desired, a paper form can be scanned and uploaded as a supporting document.

Once questionnaires are submitted, they are immediately available for review. At any time thereafter, respondents may access their submitted questionnaire to review and, if desired, revise their answers. The system retains both the original and the revised answer.

The system includes a document library where the client can make their policies, procedures, forms, etc. available for access by respondents and reviewers.

Questions can be designed so that any particular response will trigger an additional question asking for more detail. Policies can be built into the question structure. For example, a client may decide that a gift of less than $50 does not require additional follow up. The system can track this item but not require that it be reviewed. Or it can be sent to a reviewer who can then simply click on a Review Action saying "No Further Action Required".

The COI-SMART LE system was designed to do more than simply manage the collection of COI Disclosures. The system is designed to manage *conflicts* that are uncovered through the disclosure process. The COI-SMART LE review process distinguishes this program from others on the market.

The COI-SMART LE review process enables and tracks detailed communication between reviewers and respondents. Correspondence may include attachments, which can be uploaded by reviewer or respondent.

A reviewer can conduct a Search to filter respondents for follow-up by department, role, disclosure status, etc.

Members of a review committee may be assigned as reviewers, or a single reviewer can forward disclosure information to committee members if desired.

The system provides comprehensive standard reports that can be exported to MS Excel. Clients also have the ability to design custom reports for an additional fee, which can be programmed and added to the list of available reports.

1.3   Administrator Guide

The purpose of this document is to describe the tools available to administrators of COI-SMART LE.

1.4   Navigation
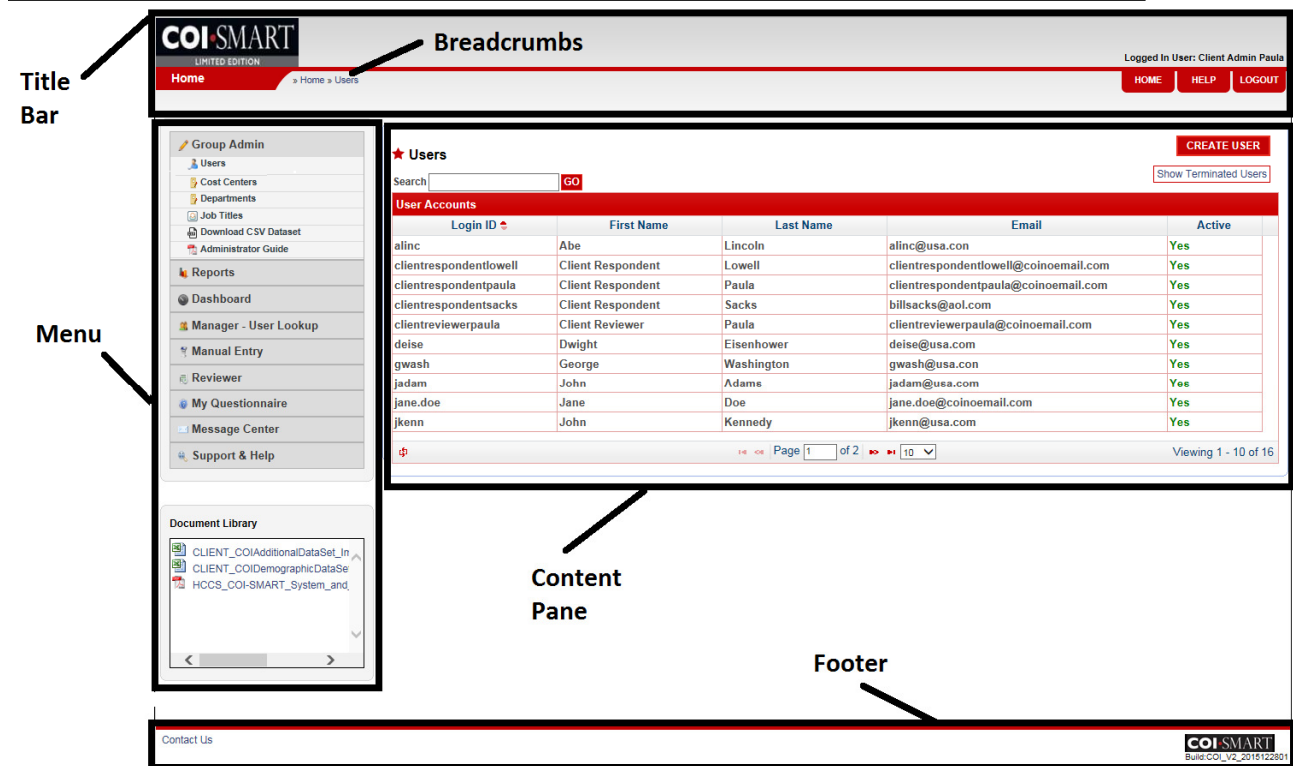
COI-SMART LE web pages are divided into sections.

Title Bar. This is where the user name is displayed. If your organization opts for it, it's also where a custom logo a can be displayed.

ⓘ *A custom logo is not included in the LE license. Your organization can utilize a custom logo for an additional fee. Contact your Account Manager for more information.*

"Breadcrumbs". This is a link that displays the current selection off the menu. Breadcrumbs offer users quick navigation links to prior screens.

Menu. This is where available functions are displayed and selected.

Content Pane. This is where the content of the menu selection is displayed. All transactions are performed in this section.

2. Account Administration

On the left navigation menu, click on Group Admin. The following sub-menu displays:
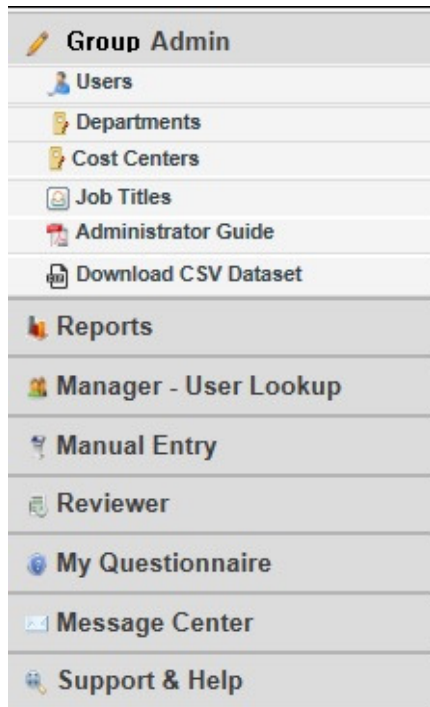
2.1 Roles

Roles are assigned to respondents to determine the questions and/or questionnaires they will receive. Roles are also assigned to questions to determine their associated respondents. Roles are also used for searching and filtering data in the reviewer queue and in reports. The COI-SMART team will work with your organization to set up and manage roles as needed.

2.2 Departments

Departments are assigned to respondents. Departments are also used for searching and filtering data in the reviewer queue and in reports.

2.3 Cost Center

A Cost Center may be a Facility, Business Unit or Tax Entity on the organization's accounting ledger. Cost centers are also used for searching and filtering data in the reviewer queue and in reports.

2.4 Permitted Values

Permitted Values are predefined lists which are shared across all questionnaires. Permitted Value Lists can be used within questions to create "drop-down" lists, or "type ahead" lists (similar to what is used in Google) to simplify and standardize responses. For example, if a question asks the respondent to identify a relationship, a drop down list can offer choices of spouse, sibling, parent, child etc. Alternatively, a list of the top ten Pharmaceutical companies might be used so a respondent can choose "Pfizer" instead of incorrectly typing "Phizer" in a text box. This way data is much cleaner and the database is a more valuable tool for "mining" and reporting data.

ⓘ *Permitted Values are not included in the LE license. Your organization can utilize Permitted Values Lists for an additional fee. Contact your Account Manager for more information.*

2.5 Email Templates

Email Templates are used to provide standardized, reusable email content for commonly sent messages to both respondents and reviewers. Email Templates are used by system-managed triggers, activated by various predefined events as outlined below.

Listed below is a description of each email template.

Expired Password	The system uses the text in this template when it triggers an email to a user upon password expiration.
Lost Password	The system uses the text in this template to send an email to the user upon clicking "Forgot Password?" on the login page.
Open Questionnaire	The system uses the text in this template to send an email to all respondents once the questionnaire's open date arrives. This email will indicate that the questionnaire is now available for response and will contain a unique link to the questionnaire. See more on emails and passwords below.
Questionnaire Reminder	The text in these templates is used by the system for sending email reminders to respondents using the fixed schedule listed below. • <u>Questionnaire Reminder 1</u> – sent to respondents 30 days after they receive the Open Questionnaire Email. • <u>Questionnaire Reminder 2</u> – sent to respondents 60 days after they receive the Open Questionnaire Email. • <u>Questionnaire Reminder 3</u> – sent to respondents 74 days after they receive the Open Questionnaire Email and re-sent once per week for the subsequent 2 weeks.
Questionnaire Submitted	The text in this template is automatically sent to a respondent as confirmation that their questionnaire was submitted successfully.
Reviewer	Email templates of this type may be sent by reviewers to support any needed correspondence.
Review Action Reminder	If a follow-up date is specified on a review action, an email will be automatically sent to the reviewer on that date using the text in this template.
Revision Notification	The system uses the text in this template to send an email to reviewers as notification that a given respondent revised their questionnaire.
Escalation Notification	The system uses the text in this template to send an email to a given assigned reviewers with a review level matching the escalated value.
Email Questionnaire	The text in this template is used by the system when emailing a PDF copy of the respondent's questionnaire responses to them upon request from the respondent.
Weekly Submission Summary	The system uses the text in this template to communicate to Administrators and Reviewers that Respondents have made submissions during the past week.

ⓘ *Your organization has the option to customize the text of several email templates from above and/or the schedule for an additional fee. Contact your Account Manager for more information.*

2.6 Job Titles

Job Title is an optional field that can be used for custom reporting. "Job Title" has no effect on the assignment of questions in the questionnaire.

2.7 Review Action Types

Review Action Types are used to determine the overall questionnaire status. The most recent review action type takes on the overall questionnaire status. Review Action Types can also be used for searching and filtering data in the reviewer queue and in reports.

Review Action Types			
ReviewActionType	Phase ⬍	Status	Visible
Internal Communication	0	Internal Communication	No
Further investigation required	3	Awaiting further investigation	Yes
Conflict Identified	4	Conflict Identified	Yes
Add to COI Meeting Agenda	20	Awaiting discussion by COI Committee	Yes
All Reviews Complete	80	All Reviews Complete	Yes
All Conflicts Managed	85	All Conflicts Managed	Yes
No Conflict Identified	90	No Conflict Identified	Yes

2.8 Security Profiles

A Security Profile is a set of access rules for users of your organization's system. Each user account on the system is assigned a single Security Profile that defines access for that user. Each user is assigned a Security Profile before they can access any screens. Each Security Profile contains the rules that dictate which screens a user can access as shown below.

Page 10 of 31

Listed below are the Security Profiles in LE:

Security Profile Name	Permissions
Administrator	All (Group Admin, Reports, Dashboard, Manager – User Lookup, Manual Entry, Reviewer, My Questionnaire, Message Center, Support & Help)
Reviewer	Reviewer , My Questionnaire, Message Center, Support & Help
Respondent	My Questionnaire, Message Center, Support & Help
Manager	My Questionnaire, Manager – User Lookup, Message Center, Support & Help

2.9 Users

The 'Users' screen provides the ability to maintain user contact and related information. Users can be searched using the Search input area. They can be sorted by any of the column names in the screen shot above by clicking on the blue column title.

Users are categorized according to a security profile: Administrators, Respondents, and Reviewers. As Respondents, they are assigned Roles for questions; they are also assigned Departments (and optionally Cost Center) for data searching and filtering in the reviewer queue and in reports.

To add a new user to the system manually, select "**Create User**" on the upper-right of the screen. To edit a particular user's demographic information, click on the user's name and then select "**Edit**" (See the section below for descriptions of each field of the selected User screen).

Other options include "Add Memo to User" "User Summary Lookup", "Delete", "Deactivate", "Terminate" or "SendEmail".

ADD MEMO TO USER	USER SUMMARY LOOKUP	EDIT	DELETE	DEACTIVATE	TERMINATE	SEND EMAIL

Click on "**Add Memo to User**". The memo functionality allows an Administrator, Manager or Reviewer (based on Security Profiles) to document respondent-specific information and communication *prior to* the respondent being assigned to or completing a questionnaire.

Click on "**User Summary Lookup**" to see if a respondent has submitted an assigned questionnaire. This view will show the respondent's assigned departments and reviewers.

Click on "**Edit**" to edit the account of the selected user.Use the "**Delete**" action when you want to remove the user from the database, including reports. This is especially useful if a respondent was added in error.

Use the "**Deactivate**" action to restrict a user from logging in while still enabling their data on reports. This feature is especially useful for respondents on leave, inactive Board Members, and others when you need to report on their disclosures for several years after they depart the Board.

Use the "**Terminate**" action when a respondent is no longer employed or affiliated with the organization and you no longer want the respondent to appear on reports. You can "Un-Terminate" the respondent if they are re-hired or if you later find that you need their data to appear on reports.

This last option ("**SendEmail**") is particularly useful when respondents claim that they have not received an automated announcement or reminder for a particular questionnaire. An Administrator can manually send a specific questionnaire announcement email to a respondent while speaking with the respondent on the phone and can ensure receipt.

2.9.1 Editing a User

To edit a particular user's demographic information from the 'User's' screen, click on the user's name and then select "**Edit**".

| ADD MEMO TO USER | USER SUMMARY LOOKUP | ✏ EDIT | ✖ DELETE | 🔒 DEACTIVATE | 🔒 TERMINATE | ✉ SEND EMAIL |

Listed below is a description of the fields displayed under the "Edit" option:

★ Edit User - Jane Doe

PRIMARY INFO
* = Required

First Name : Jane *
Middle Name :
Last Name : Doe *
Email : jane.doe@coinoemail.com *
Login ID : jane.doe *
Job Title :

SECONDARY INFO

Phone Number :
Fax Number :
Address :
City :
State :
Zip :
Comments :
Location :
Section :
National Provider Identifier (NPI) :
Employee ID :
SSN :

Primary Info -

      First Name. User's First Name. *Required*.

      Middle Name. User's Middle Name.

      Last Name. User's Last Name. *Required*.

      Email. User's email address. This is a unique identifier for the user. *Required*.

      ⓘ *If an email address does not exist, use firstname.lastname@coinoemail.com as a placeholder until a valid email address can be entered. The system will not send announcements and reminders to emails with the domain name: coinoemail.com.*

Login ID. User's Login ID. *Required*. Some clients use email address for Email AND for username.

Job Title. Select from a drop-down list. Optional, however, this may be used for 990 reporting. The Job Title selection tool is only available if a Job Title has been defined in the "Job Titles" administration tool or added through the user demographic data file.

Job Title: Billing Staff ▼

Secondary Info -

Phone Number. User's phone number.

Fax Number. User's fax number.

Address. Work or residence address.

City. Work or residence city.

State. Work or residence state.

Zip. Work or residence zip Code.

Comments. Notes.

Location. Facility or Ship-to

Section. Lot or Division

National Provider Identifier. This field is reserved for National Physician/Provider ID which may be used in the future in conjunction with the provisions of the Physician Payment Sunshine Terms of the Affordable Care Act. Optional.

Employee ID. User's Employee ID. Optional.

SSN. User's Unique ID. Optional. Clients are encouraged **not** to input Social Security Number. This field is provided for legacy purposes from a previous version of the system. You may use this field for additional identifiers.

Security Profile -

SECURITY PROFILE

* = Required

Security Profile : Respondent ▼ *

Security Profile. Select from a drop-down list. *Required*.

ⓘ *For more information of Security Profiles, see "2.8 Security Profiles".*

Miscellaneous Settings -

Force Password Change. Check this flag to expire a user's password immediately.

Super Reviewer. Check this option to provide a user access to review all questionnaires, regardless of Role.

Locked. This option will be automatically selected if users mistype their password more than five times in three consecutive minutes.   The selection means that the user will be temporarily unable to log in. The option will be automatically deselected after 30 minutes. You can manually deselect this option to enable the user to re-attempt to log in if they call for assistance before the 30 minute timeout.

ⓘ *This option may be used to manually lock a user out of the system. With a manual lock, the system does not automatically deselect after 30 minutes. To prevent a user from logging into the system, use the "Active" setting below.*

Active. User's status. If not active, the user will not be able to log in.

Beta User: Check this option to allow user access to a questionnaire that is in Beta Mode

Role Assignments -

Role. Select from a list box. You can select more than one role. *Required.* Selections made here by the Administrator cannot be de-selected in the "My Profile" page by respondents. Similarly, Role selections pre-set by demographic upload files may not be de-selected in the "My Profile" page by respondents.

Department Assignments -

Departments. Select from a list box. You can select more than one department. *Required*.

This controls how reports are generated and how reviews the respondent's question.
Notes:
1. Although a primary department can be set here, the demographic upload process will create a new primary department; the previous primary department will become secondary.
2. Administrators can allow respondents to self-select secondary departments on their My Profile page. See Settings under Account Admin.

Primary Department. Select from a drop-down list. Primary Department is used in standard reporting. *Required*.

Cost Center Assignments -

Cost Center. Select from a drop-down list. *Optional.* Cost Center will only display if Cost Centers have previously been created via batch upload files.

ⓘ A planned enhancement will allow an administrator to manually create Cost Centers so they will be visible in this screen.

Password -

Change Password. Click this link to reset a user's password. *Optional*.

ⓘ The field will expand as shown in the screen shot below.

New Password and **Confirm Password**. Enter the same value for both fields following the schema shown above.

2.9.2 Adding a User

To add a new user to the system manually, select "Create User" on the upper-right of the 'Users' screen.

ⓘ *See the "2.9.1 Editing a User" section above for a description of each field. Refer to the notes below with regards to setting a password for new users.*

> **Password** and **Confirm Password**. When creating a new user in the Admin Account / Users area, two additional Password fields will be shown: **Password** and **Confirm Password**.

> You may leave the password section blank. The Respondent will have the opportunity to create their own password once they receive their Open Questionnaire Email. If you create a password for the Respondent, you will need to communicate the password you set on this screen to the user, either by phone, email or some other method outside of the COI-SMART LE system.

Users who are created in bulk via automated demographic upload files will have no password assigned to them. When a questionnaire is ready for one of these users, a unique email will be sent to them containing a custom link, enabling them to set their own password before logging in.

ⓘ *For information on user's first-time password setting and COI-SMART LE links embedded in announcement emails, please see the "3.2.2 Custom URL" section in the Troubleshooting section of this guide.*

ⓘ *When editing a previously-created user's account, you cannot see their password, however, you can reset it by clicking the "Change Password" link on the bottom-right of the screen.*

ⓘ *For more information on passwords, see the "3.2.2 Security" section in the Troubleshooting section of this guide.*

3. Troubleshooting Guide

3.1 Supported Browsers

COI-SMART LE supports the following browsers:
➢ Microsoft Internet Explorer version 9 or higher on Windows
➢ Mozilla Firefox version 2 or higher on Windows and on Apple OSX or higher
➢ Apple Safari version 3 or higher on Apple OSX or higher

ⓘ *Respondents have reported success with smart phones (iPhone, etc.) and tablets (iPad, etc.); However, these platforms are not officially supported by HCCS.*
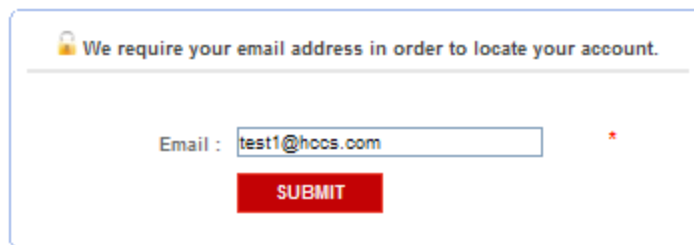
3.2 Logging In / Passwords

3.2.1 Direct URL

As administrator, go to the direct URL: https://*client*.coi-smart.com.
Where ***client*** is the subdomain name assigned to your institution.

Enter your user name and password. To reset your password, click the 'Forgot Password' link. The following screen appears:

Enter your email address. Follow the instructions on the email to log into the system.

3.2.2 Custom URL

The direct URL also works for respondents and reviewers. However, some respondents and reviewers may have received an email with a custom link to log into the system, for example:

https://*test*.coi-smart.com/password_reset.php?a=onDiDg88T6rHFlLDL7pbhA%3D%3D&b=MIANDcANB73SAl2sIOuCIA%3D%3D

By clicking on the custom link, the system automatically directs the user to one of two pages:

a) Login page (if a password exists)

b) Set Password page (for first-time users)

A note on first-time password setting and COI-SMART LE links embedded in an announcement email.

We designed the questionnaire announcement and password feature to work in the same way facebook™ works. Before a questionnaire announcement is sent to a respondent, the database checks if they have a password set. If the respondent does not already have a password, the link embedded in the announcement email contains a unique, one-time-use link. When the user clicks the link, they are brought to a special login page, unique to them, and asked to set their own password (see screen shot "b" above). Since the link embedded in the email is unique, and since the system trusts that only the named respondent has access to their own email, no other user can get to that page in the COI system.

Here is a sample of an announcement to a respondent that has not previously set a password. Note the long, unique link in the email:
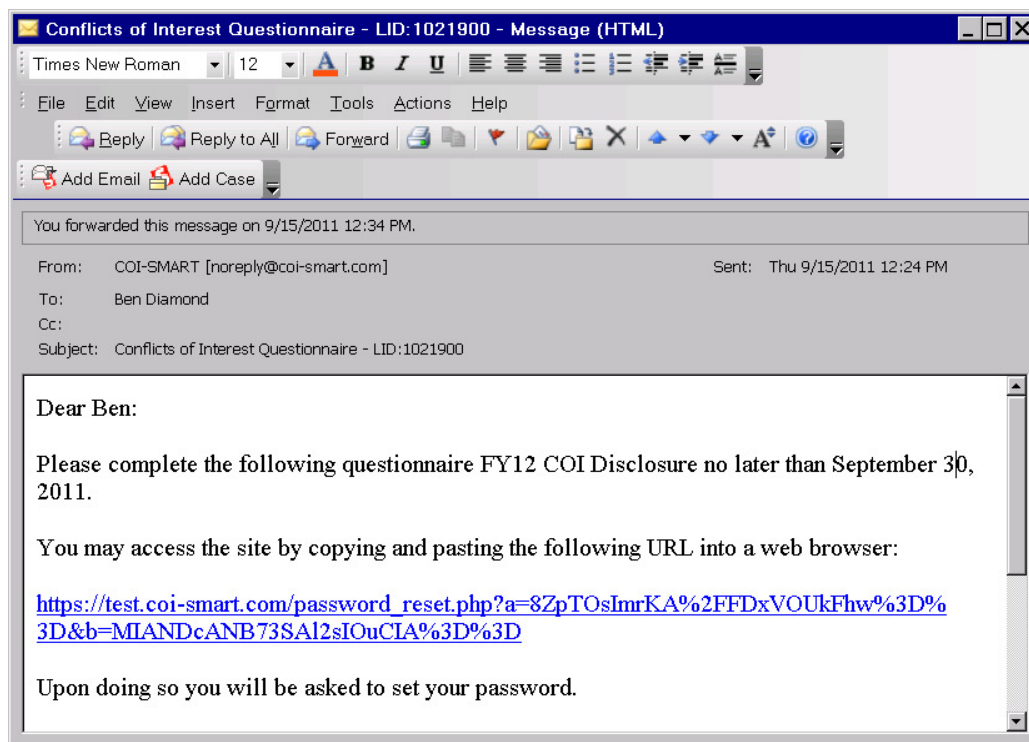
When the respondent clicks on the embedded link, they are brought to the set-password screen (screen shot "b" above).

If the link is used again (say the user clicks it a week later), the system knows that a password has already been set and brings the user to the login page (screen shot "a" above), requiring their ID (which is in the announcement email) and the password they previously set. If they forget their password, they can use the "Forgot Password" link, which generates a new unique link email to them.

Because the link is unique to each respondent, DO NOT cut and paste your unique link and email it to others.

If the respondent has previously set a password, the link in the announcement email will look different. It will contain only the domain name. In the example email above, the link might be https://test.coi-smart.com

3.2.3 Security

The system locks the user's access after more than 5 password attempts in 3 minutes. It unlocks the user after 30 minutes. The administrator can also go into the user's record and clear the Locked flag.

For general troubleshooting, the administrator can perform the following steps:

1. Ask the user to wait 30 minutes and try logging back in.

2. If 30 minutes has passed, resend the announcement email. On the Menu, select "Account Admin" -> "Users". Select the user and click "Send Email". The user will be sent an email with the custom link.

3. To reset a user's password, click the "Change Password" link at the bottom of the User page.
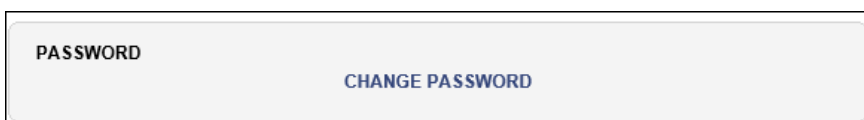
ⓘ The field will expand as shown in the screen shot below.

New Password and **Confirm Password**. Enter the same value for both fields following the schema shown above.

3.2.4 Password / Reset Password

If a user forgets their password any time after they set it, they can reset it by selecting the "Forgot Password" link on the login screen and typing in their email address.

After they hit "Submit" on the form, an email will be sent to them with a new unique URL, similar to the example shown in 3.2.2 ("Custom URL") shown above.

3.3 Manual Entry

Administrators can enter and view data on behalf of the respondent. From the Menu, select 'Manual Entry' -> 'Start Manual Entry'.

A list of all registered users will display. Select the user and click 'Complete A Questionnaire For This User'. The 'My Questionnaire' page will display for that user.

Manual Entry is used if the respondent could not log into the system due to limitations. More likely, the respondent has filled out a paper form, which needs to be transcribed into the electronic version. If desired, the paper form can be scanned and uploaded into the questionnaire as a supporting document.

The ability to perform Manual Entry is assigned to the Administrator Security Profile by default.

ⓘ *As a general recommendation, Administrators (or those performing Manual Entry) should scan a copy of the respondent's paper questionnaire and attach the scanned document to the first question in the questionnaire. This will serve as future proof of the paper response.*

3.4 Reports and Dashboards

3.4.1 Reports

The system has a robust reporting engine that track the cycle from response to review. To access the reports from the Menu, click 'Reports' -> 'Reports'
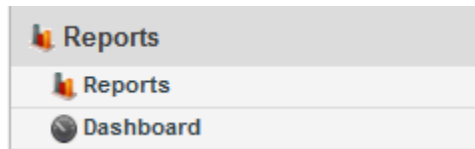
There are 10 standard reports that can be exported to MS Excel.
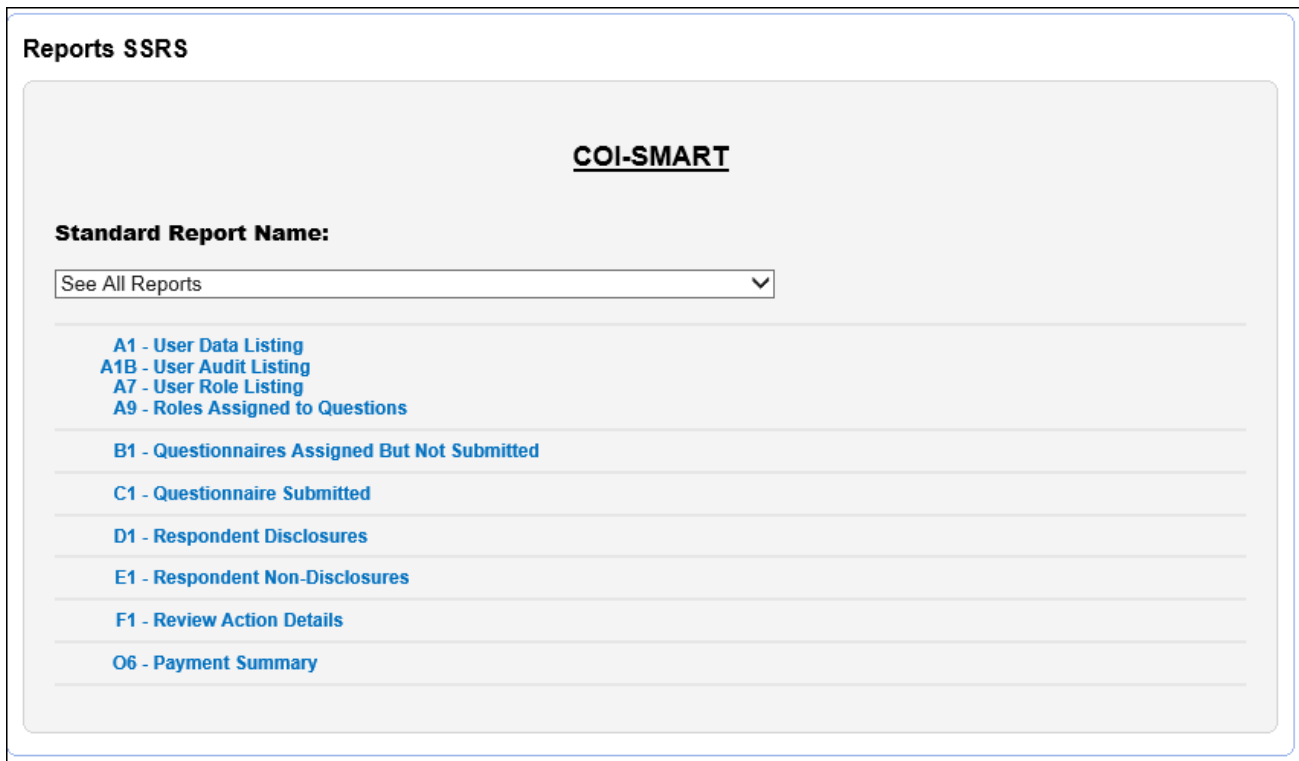
Depending on the report, a filter screen will appear. Choose a filter option (e.g. Questionnaire Name, Department, Role), then click 'OK'. If no filter is desired, click on the X next to the filter type to delete it, then click 'OK'.

If no data is available, the message "No Data Qualified" will appear.

3.4.2 Dashboards

Dashboards are designed to provide insight into specific questionnaire criteria at a particular point in time. Currently, there are three available dashboards: Percent of Assigned Questionnaires Received, and Review Status Summary, and Disclosures by Risk Area.
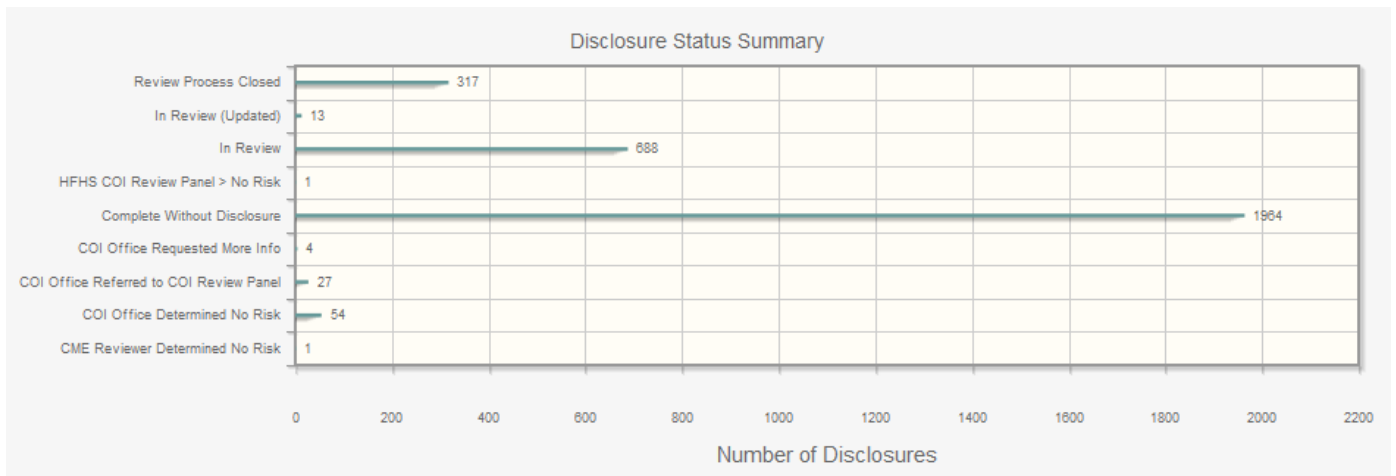
Percent of Assigned Questionnaires Received

This dashboard shows the percentage of questionnaires received out of the total number of questionnaires assigned at a specific point of time.
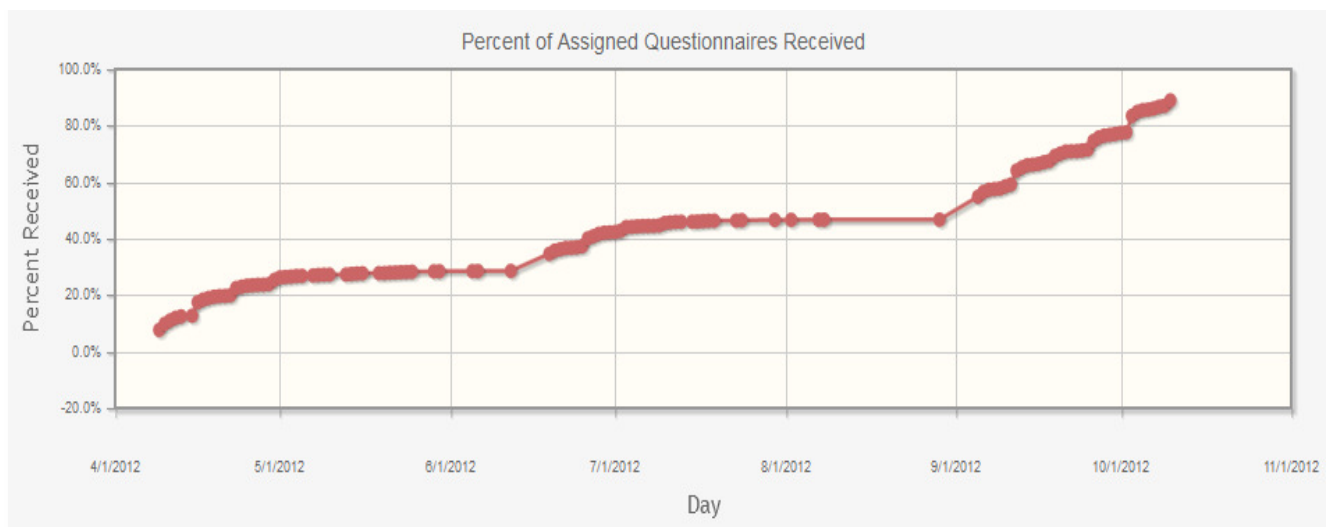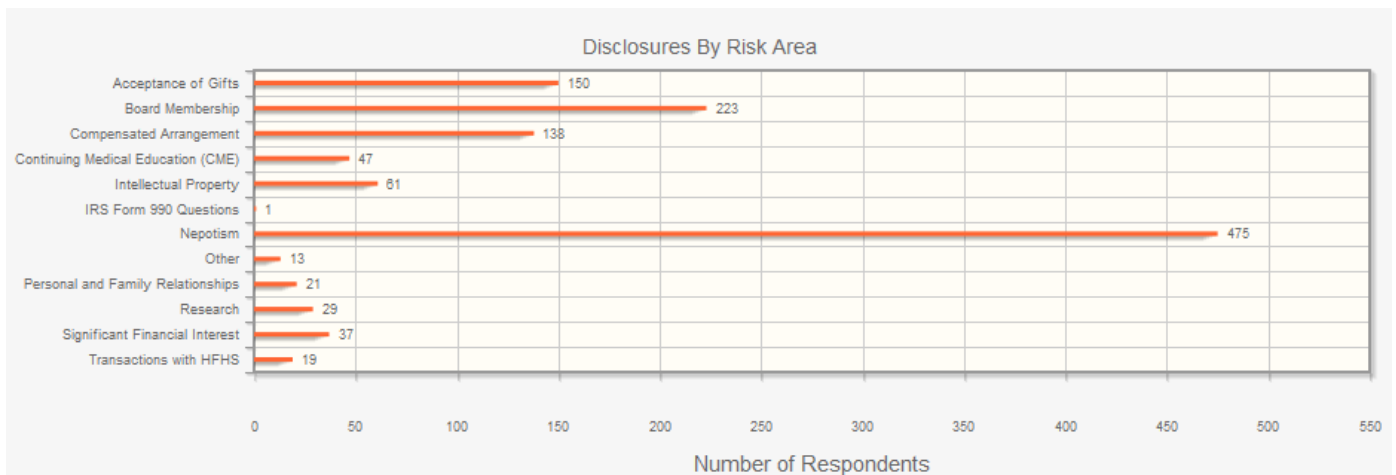

Review Status Summary

This dashboard shows the number of disclosures per disclosure status (review status) at a specific point in time.

Disclosures by Risk Area

This dashboard shows the number of disclosures per risk area (question category) at a specific point in time.

Appendix. Standard Reports

A1. User Data Listing. Report displays demographic information from the user's profile.

Fields: Organization ID, Email address, First Name, Middle Name, Last Name, Comment Text, Primary Department, Section, Location, Cost Center, Phone, Address, City, State, Zip, Fax, SSN, National Provider ID, Job Title, Employee Status, Login Name.

Filter: none

NOTE: This report may be used as a template by an Administrator to download current active users, then add new users and/or deactivate users from the spreadsheet and send the file back to HCCS. The format is required for HCCS to quickly and accurately process any returned files.

A1B. User Audit Listing. Report displays some demographic information and additional administrative data

Fields: LoginID, LastName, FirstName, MiddleName, Email Address, User Status, SSN, Job Title, Primary Department, Cost Center, User Creation Date, Password Changed Date, Locked, Super Reviewer, Security Profile

Filter: none

A7. User Role Listing. Report displays all registered users and assigned role(s)

Fields: Organization ID, LoginID, LastName, MiddleName, FirstName, User Status, Role, Role Assignment Date, Role Type

Filter: none

NOTE: Users can be assigned to multiple roles.

A9. Roles Assigned to Question. Report displays roles assigned to questions

Fields: OrganizationID, Questionnaire, Question #, Group #, Role

Filter: Questionnaire name

NOTE: Report includes both published and beta questionnaires

B1. Questionnaire Assigned But Not Submitted - Report displays all respondents that have not completed their assigned questionnaire(s). It also lists respondents whose questionnaires are "in progress" status.

Fields: Questionnaire, Respondent, User Status, User ID, Primary Department, Email Address, Phone Number, Questionnaire Open Date, Email Sent Date, Days Elapsed, <=30, >30 and <=60, >60 and <=120, >120

Filter: Questionnaire

C1. Questionnaire Submitted. Report displays all respondents that have completed a questionnaire.

Fields: Questionnaire, User ID, Respondent, User Status, Primary Department, Most Recent Submission Date, Disclosure, Filing Year

Filter: Questionnaire, Submission Date

D1. Respondent Disclosures. Report displays all responses that are marked as reportable.

Fields: Questionnaire, User ID, Respondent, User Status, Question #, Revision, Entity, Group, Question, Sub-Question, Response, Last Submission Date

Filter: Questionnaire, Submission Date

E1. Respondent Non-Disclosures. Report displays all responses that are not marked as reportable.

Fields: Questionnaire, User ID, Respondent, User Status, Question #, Revision, Entity, Group, Question, Sub-Question, Response, Last Submission Date

Filter: Questionnaire, Submission Date

F1. Review Action Details. Report displays all respondents, their disclosures, and corresponding review actions.

> Fields: Questionnaire, User ID, Respondent, User Status, Primary Department, Question #, Question, Last Submission Date, Phase, Status, Review Level, Reviewer Name, Review Type, Comment, Last Comment Date
>
> Filter: Questionnaire, Submission Date

O6. Open Payments - Payment Summary. Report displays a summary of payments to providers reported by pharmaceutical and device companies to CMS.

ⓘ Provider NPI Numbers must be loaded in demographics to provide results.