Colorado Regional Health Information Organization

Participant Procedures

TABLE OF CONTENTS

COMPLIANCE WITH LAWS AND POLICIES

About CORHIO

CORHIO is a nonprofit, public-private partnership that is improving health care quality for all Coloradans through cost effective and secure implementation of health information exchange (HIE). CORHIO is designated by the State of Colorado to facilitate HIE.

CORHIO Policies

CORHIO and each Participant shall, at all times, comply with all applicable CORHIO Policies. The CORHIO Policies may be revised and updated from time to time, and such, revisions and updates shall be effective upon notice to Participants, as specified in the Participant Agreement(s). Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these CORHIO Policies.

APPROPRIATE USE AND DISCLOSURES

Procedure: CORHIO HIE User Agreement and Appropriate Use of Services

PURPOSE

To ensure that Participants of the CORHIO Health Information Exchange (HIE) are aware of and acknowledge acceptance of the rules for accessing protected health information (PHI) using the CORHIO HIE's PatientCare 360 system. The rules for accessing PHI – called the User Agreement and Appropriate Use of Services – are based on CORHIO's Privacy and/or Security policies and procedures; state and federal confidentiality laws and regulations including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

SCOPE

This procedure applies to the Participant and CORHIO project teams for training purposes

PROCEDURE

Upon initial login to the PatientCare 360 application, each user will be required to electronically acknowledge acceptance of the User Agreement and Appropriate Use of Services included here as Appendix A.

In the event the agreement is amended, each user will be required to acknowledge the amended
Agreement upon the next login to the application following the amendment.

Acknowledging the User Agreement is an event audited by the system.

"ACCESS ADDITIONAL RECORDS" ACCEPTANCE PROCEDURE

Each time a user selects "access additional records" in PatientCare360 to obtain patient information for which the user is not designated as the provider of the record, the user will be required to electronically acknowledge acceptance of the associated Confidentiality Agreement included here as Appendix B.

Accessing additional records and acknowledging the Confidentiality Agreement are events audited by the system.

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
3/1/2011	1.0	Kelly Joines	Original Document
1/9/2012	1.1	Patty Cerna	Changed language to reflect current process for EULA signature and review of the Break Glass Confidentiality statement
3/29/2012	1.2	Kelly Joines	Updated to reflect access of PHI through the CORHIO PatientCare 360 application.
7/6/2015	1.3	Janeece Lawrence	Updated to make name change from break glass to access additional records

APPENDIX A - USER AGREEMENT AND APPROPRIATE USE OF SERVICES

As a condition to being allowed access to the CORHIO Health Information Exchange ("the System"), I agree to abide by the following terms and conditions:

1. I will not disclose my user name and password to anyone.

2. I will not allow anyone to access the System using my user name and password.

3. I will not attempt to learn or use another's user name and password.

4. I will not access the System using a user name and password other than my own.

5. I am responsible and accountable for all data retrieved and all entries made using my user name and password.

6. If I believe the confidentiality of my user name and password has been compromised, I will immediately notify the CORHIO help desk so that my password can be changed.

7. I will not leave my computer unsecured while logged into the System.

8. I will treat data available to me through the System confidentially, as defined by HIPAA. I will not disclose any confidential information unless required to do so within the official capacity of my job responsibilities, and then limited to parties with a legitimate need to know.

9. I will not access, view, or request information regarding anyone with whom I do not have a clinical relationship or a need to know to perform my job responsibilities. I acknowledge that my use of the System will be routinely monitored to ensure compliance with this agreement.

I further acknowledge that if I violate any of the terms as stated above, I am subject to loss of System privileges, legal action, and/or any other action available to CORHIO.

APPENDIX B – "ACCESS ADDITIOLNAL RECORDS" AGREEMENT

CONFIDENTIALITY ALERT

You are trying to access patient information for which there is no current system data showing you to be a provider of record. Permitted uses of the information are for treatment and payment purposes for patients which the user has a direct and active treatment/care provider role or has been requested to perform a consultation by the physician who is the primary care provider for the patient. You can establish this relationship as either longer term or for one time access by choosing the appropriate option below.

PLEASE BE ADVISED THAT ACCESS TO ALL PATIENT RECORDS IS TRACKED THROUGH AN AUDIT PROCESS. INAPPROPRIATE ACCESS IS A CRIMINAL OFFENSE THAT COULD BE A CLASS D FELONY THAT IS PUNISHABLE BY 8 YEARS IMPRISONMENT, FINES AND PENALTIES FOR EACH OFFENSE AND IMMEDIATE TERMINATION OF CORHIO ACCESS.

PROGRAM OPERATIONS

Procedure: CORHIO Health Information Exchange (HIE) Maintenance – Communication Plan

PURPOSE

To define key CORHIO communication activities and events related to the Health Information Exchange (HIE) prior to and after the Participant is live on HIE.

SCOPE

This procedure applies to the Participant Organizations and CORHIO.

OBJECTIVES

Objectives of the HIE Maintenance Communication Plan are as follows:

- Define CORHIO roles and responsibilities for communicating events and policy and procedure modifications to Participants.
- Document any assumptions or risks associated with communicating events to Participants.
- Define key communication events that need to be shared with Participants, including responsibilities, medium and frequency of communication.

ROLES AND RESPONSIBILITIES

The following are key roles and responsibilities for communicating key events to Participants:

Role	Primary Responsibilities
CORHIO	
CORHIO Service Desk	Responsible for communicating key events and policy and procedure modifications to Participants once they have transitioned to Support.
CORHIO Program and Project Managers	Responsible for communicating key events and policy and procedure modifications to Participants during the project implementation period.
Security Response Team	• Primarily responsible for disseminating communications related to Security Events to Participants and assigning communication responsibilities to CORHIO team. • Coordinates key messages and resolutions to share with Participants related to the Security Events.
Policy Committee Liaison	• Primary point of contact between CORHIO and the Policy Committee. Specifically related to updates and changes communications between the two groups.
CORHIO Vendors	
Project Team	Work with CORHIO on communication messages and resolutions.

Role	Primary Responsibilities
Participant	
Participant Contract Owner	• Responsible for receiving designated communications and disseminating communication to necessary Participant parties. • Works with CORHIO on next steps and resolution of communication event, if necessary.
Participant Point of Contact	• Responsible for receiving designated communications and disseminating communication to necessary Participant parties. • Works with CORHIO on next steps and resolution of communication event, if necessary.
Participant Security and Privacy Officer	• Responsible for receiving designated communications and disseminating communication to necessary Participant parties. • Works with CORHIO on next steps and resolution of communication event, if necessary.
Help Desk End Users	Receives designated communications from CORHIO.

ASSUMPTIONS AND RISKS

Assumptions

The following are assumptions related to CORHIO communications:

Assumption	Description
The CORHIO Project Team and Service Desk will be primarily responsible for disseminating necessary communication events.	The Program/Project Manager and/or the Service Desk Lead will assign necessary communication tasks to the appropriate CORHIO team. A back up will be assigned to address any out of office coverage as necessary.
Communication events can be discovered by any HIE stakeholder or party.	Communication events may be discovered by internal CORHIO employees, Participants, patients, and additional HIE stakeholders.
This list defines communication events captured upon the initial creation of this document. Additional events may be uncovered.	As the HIE becomes more widely used, additional communication events may be discovered. This document will be updated to reflect additions and changes.

Risks

The following are risks related to CORHIO communications:

Risks	Mitigation Plans
If the Maintenance Communication Plan is not followed internally, key communication events may not be disseminated to Participants.	The Program/Project Manager and/or Service Desk is primarily responsible for ensuring the Maintenance Communication Plan is executed.

COMMUNICATION EVENTS AND MAINTENANCE

The following table outlines the key communication events and activities related to HIE Maintenance.

Deliverable	Purpose	Delivery Method	Frequency	Owner	Audience
Policy Updates	Deliver revised policies to internal and external stakeholders.	• Email • Help Desk Announcements • Add release to FAQs	As needed based on yearly review	• Program/Project Manager • Service Desk • Policy Committee Liaison	• Participant Contract Owner • Participant Point of Contact • Help Desk Users • Policy Committee • CORHIO Employees
Procedure Updates	Deliver revised procedures to internal and external stakeholders.	• Email • Help Desk Announcements • Add release to FAQs	As needed based on yearly review	• Program/Project Manager • Service Desk	• Participant Contract Owner • Participant Point ofContact • Help Desk Users • CORHIO Operations
System Upgrades and Release Notifications	Communicate system upgrade information, including planned system outages, and technical details, including release notifications.	• Email • Help Desk Announcements • HIE Announcements • Add release to FAQs	As needed based on release schedule	• Service Desk	• Participant Point of Contact • Help Desk End Users • CORHIO Operations • HIE End Users
Critical Issues	Communicate critical issues, including unplanned system downtime or outages to HIE users, patient safety, or other critical issues.	• Email • Help Desk Announcements • HIE Announcements	As needed	• Service Desk	• Participant Contract Owner • Participant Point of Contact • Help Desk End Users
Security Event Notifications	Communicate any security event or notification to necessary stakeholders.	• Phone • Email, as needed	As needed	• Security Response Team	• Participant Security and Privacy Officer

REVISION HISTORY

Version	Date Issued	Updates Includes
V1.0	1/1/2011	Initial Publication
V1.1	3/1/2011	Updated Communication Events Table
V1.2	5/1/2011	Updated CORHIO Roles and Responsibilities to distinguish between activities that occur before and after participants have been transitioned to ongoing implementation support.

Procedure: CORHIO Investigating Participant HIE System Misuse

PURPOSE

CORHIO maintains strict policies and procedures to ensure appropriate and authorized use of the CORHIO System. Each Participant shall allow access to the CORHIO System only by those Workforce Members who have a legitimate and appropriate need to use the CORHIO System or release or obtain information through the CORHIO System. No Participant Workforce Member shall be provided with access to the CORHIO System without first having been trained on CORHIO policies and procedures. All authorized users are responsible for all actions performed under their credentials.

CORHIO will initiate the appropriate sanctions against Authorized Users who misuse the CORHIO System in violation of CORHIO's policies and procedures.

SCOPE

This procedure applies to all Participant Workforce Members, CORHIO Leadership, CORHIO Compliance, Privacy and Security Officers.

POLICY

Failure to comply with CORHIO policies and procedures pertaining to CORHIO System use may result in disciplinary action against the Participant Workforce member committing the violation.

PROCEDURE

Each Participant shall implement procedures to discipline and hold their Workforce Members accountable for ensuring that they do not access, use, disclose or request information or data for any purpose except as permitted by CORHIO policies and procedures.

Examples of misuse include but are not limited to:

- Allowing others to access CORHIO Systems with their password
- Accessing CORHIO Systems for any purpose other than legitimate and appropriate need and as defined by CORHIO policies and procedures
- Copying or compiling data through CORHIO Systems with the intent to sell or use for personal gain

CORHIO may periodically activate, facilitate, or conduct system audits to review user or system activities.

- Random audits will focus on record held by CORHIO System and shall be conducted by CORHIO or a CORHIO authorized independent third party
- CORHIO shall notify the relevant Participant of any inappropriate use, privacy, or security breach identified through audits

The Participant shall be responsible for notifying the CORHIO Service Desk of any changes in Authorized Users including those who no longer have a legitimate need to access the CORHIO System as a part of their duties.

- If a change relates to an Authorized User who has been sanctioned for accessing, using, disclosing, or requesting PHI not permitted by CORHIO policies and procedures or non-compliance with CORHIO policies and procedures, the notification shall occur immediately and under no circumstances, in no more than 24 hours.
- If the change is unrelated to non-compliance with CORHIO policies and procedures, notification shall include updating the Authorized User status as soon as possible, within a maximum of 72 hours.

The following process will be followed when a Participant Workforce member has violated or is suspected of violating CORHIO policies and procedures:

Investigation: The CORHIO Security Response Team will conduct an investigation in alignment with the level of the violation and in accordance with the Participant's internal policies. Findings will be documented and reported to the Participant's Compliance Officer or other designee who will work with the CORHIO Security Response Team to determine the appropriate disciplinary action to impose. Depending on the investigation, CORHIO may also sanction the workforce member, disallowing access to the HIE.

Duty to Report: Any Participant Workforce member who observes, becomes aware, or suspects an unauthorized use or disclosure of PHI is required to report his or her suspicion as soon as possible to the Participant Compliance Officer or other designee. The Participant Compliance Officer or other designee will report the occurrence to CORHIO Service Desk. The Service Desk will notify the CORHIO Security Response Team which will initiate an investigation.

No Retaliation: CORHIO will not retaliate against any Participant Workforce Member who acts in good faith in the reporting of suspected misuse of the CORHIO system.

DOCUMENTATION REQUIREMENTS

All Participant Workforce Member sanctions regarding misuse of the CORHIO system will be documented and retained in a log maintained by CORHIO Security Response Team for a period for six (6) years. Documentation will include:

- Participant Workforce Member Name
- Participant Organization Name
- Description of Violation
- Location of Violation
- Date of Violation
- Disciplinary Action Taken

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
12/8/2010	1.0	Susan Clark	Original Document
7/8/2011	1.1	Kelly Joines	Clarified focus of the procedure on participant workforce; Changed title from "CORHIO Sanctions for Participant Misuse" to "CORHIO Investigating Participant HIE System Misuse" to be more in line with the policy
3/29/2012	1.2	Kelly Joines	Modified "Help Desk" to read "Service Desk." Updated Copyright
2/6/2014	1.3	Robert Denson	SRT Review

PRIVACY PRACTICES

Filtering Sensitive Data – An Overview

PURPOSE

The purpose of this document is to outline how special protection category data (sometimes also referred to as sensitive data) should be handled in an HIE setting.

BACKGROUND

This document has been created based on CORHIO's Governing Principles and Policies which state that certain patient data must be filtered by participants so that it is not available in the HIE:

Some Patient Information may be subject to special protection under Law (e.g., substance abuse, mental health, and HIV status). Each Data Provider shall determine and identify what information is subject to special protection and withhold such information as they see fit. Each Data Provider is responsible for complying with such Law.

This document does not attempt to specifically outline the law, but instead, serves as an information overview based on the current list of special protection categories. Participants are responsible for their own adherence to all pertinent law, as described in CORHIO's Governing Principles and Policies.

SPECIAL PROTECTION CATEGORIES

Genetic Information

Genetic Information cannot be used by health plans to discriminate for underwriting purposes, as set forth in the federal Genetic Information Nondiscrimination Act of 2008 (GINA). Under Colorado law, specific patient authorization is required to use genetic information for purposes other than diagnosis, treatment, or therapy. Because the CORHIO HIE is currently used for clinical data exchange and not for health plan or claims information exchange, genetic information is disclosable in the exchange as normal PHI for diagnosis, treatment, or therapy, and does not need to be filtered.

Sexually Transmitted Diseases

Information regarding sexually transmitted diseases (e.g., HIV status) is treated as PHI under the federal HIPAA Privacy Rule and should be protected as any other PHI. Colorado follows the federal rule, treating this information as other medical information. Therefore, this information is disclosable in the exchange by healthcare providers as normal PHI and does not need to be filtered.

MENTAL HEALTH INFORMATION

The HIPAA Privacy Rule creates a special category of mental health information within PHI called psychotherapy notes – records of communications during therapy sessions. These must be separated from the rest of the individual's medical record. Based on this, psychotherapy notes must be flagged by providers and filtered from the HIE. In Colorado, disclosure of any information associated with

mental health treatment requires specific patient authorization. Therefore, providers must follow their existing processes of obtaining disclosure consent from their patients before sharing this information. Therefore, as long as this process is followed, mental health information is considered normal PHI for disclosure in the HIE.

SUBSTANCE ABUSE

Substance Abuse and Mental Health Services Administration (SAMHSA) regulations severely limit the disclosure of individual information without specific patient consent by drug and alcohol treatment programs that receive federal assistance. Colorado calls for the same level of confidentiality as required by the federal regulations. Therefore, patient data from drug and alcohol treatment programs must be filtered from the HIE.

PHI UPON INDIVIDUAL REQUEST (SERVICES PAID OUT OF POCKET)

Under the HITECH rules, patients can request restrictions to prevent disclosure to a health plan of any PHI related to services that the patients pay for out of pocket. Colorado calls for the same level of PHI protection as found in the federal regulations. Because the CORHIO HIE is currently used for clinical data exchange and not for health plan or claims information exchange, PHI related to services paid for out of pocket is disclosable in the exchange and does not need to be filtered.

Procedure: CORHIO Patient HIE and Opt In/Out Notification Procedures

PURPOSE

The purpose of this procedure is to define how the Sample Patient Notification, the CORHIO Heath Information Exchange (HIE) Opt In Request Form, and the CORHIO Heath Information Exchange (HIE) Opt Out Request Form are provided to HIE Participants.

SCOPE

This procedure has been created in response to the Privacy Practices and Patient Participation and Control of Information policy that CORHIO must follow. According to this policy, CORHIO must provide Participants with a sample patient notification document (the "CORHIO Notice") that complies with applicable law and the Policy.

Procedure: Providing Documents to Participants

As part of CORHIO's process of readying a Participant to go live with HIE, CORHIO will provide the Participant with:

- Sample Patient Notification document
- Sample Opt Out form
- Sample Opt In form

In addition, CORHIO will provide an overview of the policy requirements, indicating that the Participant must provide notification to its patients that the Participant is participating in the HIE, and, unless the patient opts otherwise, the patient's clinical data will be included in the HIE. CORHIO resources will work with each Participant to determine the best approach for incorporating the policy into their unique workflow.

The Participant may choose not to use the samples provided by CORHIO. However, the Participant must abide by the defined policy to provide notification and the ability for patients to Opt Out of the HIE and to Opt back in to the HIE.

The CORHIO team will be responsible for distributing the necessary policies, procedures, and sample forms, and checking in with the Participant as part of the defined implementation activities and plan to ensure that the patient notification procedures have been operationalized before go live.

PROVIDING INFORMATION ON CORHIO'S WEBSITE

CORHIO will include information on its website directed at patients, explaining how they may Opt Out from the CORHIO HIE. This information will direct the patient to his/her care provider to determine if the provider is participating in the HIE. If that provider is participating in the HIE and the patient wishes to Opt Out, the patient will be instructed to obtain the CORHIO Health Information Exchange (HIE) Opt Out Request Form from his/her provider.

Conversely, if the patient has previously opted out and now wishes to opt back in to the HIE, the CORHIO website will direct the patient to contact his/her provider for a CORHIO Heath Information Exchange (HIE) Opt In Request Form.

THE PATIENT OPT-OUT PROCESS

Once a patient completes the Participant's Opt-Out Form, the Participant's POC shall submit this form to the CORHIO Service Desk. The CORHIO Service Desk will complete the Opt-Out transaction and save a copy of the Opt-Out form for auditing purposes. Methods of submitting Opt-Out forms are as follows:

- Emailing the Opt-Out form via encrypted email to optout@corhio.org
- Attaching the Opt-Out form to the PHI field in a ticket using the CORHIO Web Desk
- Faxing the Opt-Out form via a Secure Fax to 720-285-3207

In addition, the Participant shall maintain a signed copy of all Opt-Out Forms received from their patients.

THE PATIENT OPT-IN PROCESS

Once a patient completes the Participant's Opt-In Form, the Participant's POC shall submit the form to the CORHIO Service Desk. Methods of submitting this form are stated in the above Patient Opt-Out Process section. The CORHIO Service Desk will complete the Opt-In transaction and save a copy of the Opt-In form for auditing purposes. In addition, the Participant shall maintain a signed copy of all Opt-In Forms received from their patients.

PATIENT REPORTING

CORHIO reserves the right to run periodic reports in the HIE to determine how many patients are Opting-Out/Opting-In. Information on these will not be distributed. CORHIO shall use the reports to gather statistical data to determine if further patient education is needed. Participants may request a copy of the Opt-Out/Opt-In report from the CORHIO Service Desk.

ONGOING REVIEW

CORHIO will continuously monitor this procedure as defined in this document to determine if patient access to the CORHIO website and/or patient access to CORHIO's Service Desk dictates a modification to this procedure.

USER AUTHORIZATION

Procedure: CORHIO Maintaining Active Authorized Users

PURPOSE

The purpose of this document is to outline the approach for maintaining a current list of all Authorized Users in the CORHIO HIE and Service Desk systems.

SCOPE

This procedure applies to the Participant Organizations and CORHIO.

PROCEDURE

Each Participant shall designate a POC to be responsible for coordinating, training, and maintaining the Participant's Authorized Users. The Participant POC shall be properly trained in creating, updating, and deactivating users in the CORHIO HIE and Service Desk system. The CORHIO Health Information Exchange system includes PHI available in the PatientCare 360 Community Health Record web portal and Referral Application, as well as Protected Health Information (PHI) exchanged electronically.

ADDING NEW AUTHORIZED USERS

During the initial implementation of the CORHIO system, the CORHIO Service Desk will be responsible for enrolling new users in the HIE and Service Desk system using the Web Based User Request Form or the Excel user Request Form. New User Request Forms are required for:

- All users needing access to the Certification and/or Production HIE environments for testing.
    - HIE Users that have been set up as Authorized Users for Certification testing do not need to submit new User Request Forms for Production HIE System use. The Participant POC shall be responsible for submitting a Service Desk ticket indicating which Certification users should be transitioned to Production users. (Follow the Adding New Authorized Users process as listed below when adding any new HIE system users to Production that were not part of Certification testing.)
- EHR Implementations: a form must be submitted to the Service Desk for:
    - All providers within the practice, whether they have access to the EHR or not, unless otherwise agreed upon.
- Community Health Record Implementations: a form must be submitted to the Service Desk for:
    - All who access PatientCare 360 Community Health Record
    - All providers within the practice, whether they access PatientCare 360 Community Health Record or not, unless otherwise agreed upon

CORHIO may audit HIE system use by Participants and users to ensure that user access is properly established.

CORHIO will provide all User Request Forms and Maintaining Authorized Users Procedure documents to the Participant POC to use when developing the Participant's internal process for creating, maintaining, and deactivating users as part of the Participant training process. The CORHIO activation and deactivation process should be added to any internal Participant on-boarding process for new employees.

CORHIO requires that each Participant utilize the Web Based User Request Form (URF) for 10 users or less and the Excel User Request Form for 11+ users. CORHIO will provide the necessary access for the Web Based URF and the hard copy Excel document during the implementation process. User access requires the authorization of the user's supervisor. All User Request Forms shall be maintained by the Participant POC. When using the Excel URF, the Participant POC shall open a Service Desk ticket advising of the new users to the HIE by attaching the document and including in the body of the ticket (or email sent to helpdesk@corhio.org) the following authorization statement "I validate that all information in this form is accurate and grant permission to add/change CORHIO access for the users listed." A scanned copy of the New User Request Form is to be attached to the Service Desk ticket. The CORHIO Service Desk shall store the User Request Form in the Service Desk system with each user's Service Desk record.

The CORHIO Service Desk shall complete the New User registration in the HIE and/or Service Desk system and assign a User Role for based on the information provided by the Participant POC. For those users accessing the PatientCare 360 web portal, the Service Desk will generate an email to the New Authorized User notifying him/her of the terms and conditions of log-in and prompt the User to create a new password.

CHANGE IN AUTHORIZED USERS

The Participant's POC shall be responsible for maintaining any change in existing user information. Changes in user information range from updates to a user name, to a change in user security. Each Participant shall develop a process for tracking all user changes for the organization. The Updated User Request Form is available to the Participant POC via the CORHIO Service Desk Ticketing System within "Knowledge Base." The Participant POC shall open a Service Desk ticket advising of the change in user information. A scanned copy of the Updated User Request Form is to be attached to the Service Desk ticket. The CORHIO Service Desk shall store each Updated User Request Form in the Service Desk system with each user's Service Desk record. The CORHIO Service Desk will assist the Participant POC in updating Authorized Users. Prior to contacting the Service Desk, the Participant POC shall complete the Participant's User Request Form with the proper user information.

Notification of Change

Within 24 hours: If the change relates to an Authorized User who has been disciplined for using, disclosing, or requesting Protected Health Information (PHI) not permitted by CORHIO Policies or non-compliant with CORHIO policies, the Participant POC shall notify the CORHIO Service Desk within 24 hours of the change and reference the CORHIO Sanctions for Participant Systems Misuse and CORHIO Inappropriate Use and Non-Compliance Reporting Procedures for the necessary

disciplinary actions. An attached copy of the Updated User Request Form shall be sent to the CORHIO Service Desk within 24 hours of the change.

Within 72 hours: If the change is unrelated to non-compliance with CORHIO Policies, notify the CORHIO Service Desk within 72 hours of the change. An attached copy of the Updated User Request Form shall be sent to the CORHIO Service Desk within 5 business days of the change.

DEACTIVATING AUTHORIZED USERS

- The Participant's POC shall also be responsible for deactivating any Authorized Users in the HIE and/or Service Desk system. There are two options for deactivating users in the CORHIO HIE system.
- Lock Out- Users can be locked out of the system upon a designated date. Example: Hospital residents will be locked out after January 1, 2015 after the completion of their residency.
- Term: Immediately deactivate users and specify a reason for deactivation for tracking/auditing purposes. Example: User John Smith deactivated due to breach of security and privacy policies.

Note: Although Users are deactivated, the CORHIO HIE system does not permanently delete users to ensure retention of user data for auditing purposes.

Each Participant shall develop a process for tracking all deactivated users for the organization. A Deactivation User Request Form is available to the Participant POC via the CORHIO Service Desk Ticketing System in "Knowledge Base." The Participant POC shall open a Service Desk ticket advising of the deactivation of a user. A scanned copy of the Deactivation User Request Form is to be attached to the Service Desk ticket. The CORHIO Service Desk shall store each Deactivation User Request Form with each user's Service Desk record. CORHIO recommends that the CORHIO deactivation process be added to any internal Participant off-boarding procedure when an employee leaves or is terminated.

If an Authorized User is terminated from the CORHIO HIE system as a result of disciplinary actions or if an Authorized User was using, disclosing, or requesting PHI not permitted by CORHIO Policies or non-compliant with CORHIO policies, the Participant POC shall work with the Participant's Security and Privacy Officer; and the CORHIO Security Response Team to define a course of action, as referenced in the CORHIO Sanctions for Participant Systems Misuse and CORHIO Sanctions for Unauthorized Use or Disclosure of PHI. If the Participant and CORHIO decide to permanently ban (or "blacklist") the User from the CORHIO HIE system, the Participant POC shall report the User and appropriate information (as defined in the User Request Form) to the CORHIO Service Desk and the user will be added to the CORHIO Blacklist Log. The CORHIO Blacklist Log is maintained in the Service Desk system. Only the CORHIO Service Desk, Security Response Team, and necessary CORHIO management shall have access to the CORHIO Blacklist Log.

In addition, the CORHIO Service Desk shall run weekly audit reports to validate that all blacklisted users are deactivated in the CORHIO HIE system. Participant POCs may request copies of the report from the CORHIO Service Desk.

Notification of Deactivation
Within 24 hours: If the deactivation is a result of disciplinary actions if an Authorized User was using, disclosing, or requesting PHI not permitted by CORHIO Policies or non-compliant with CORHIO policies, the Participant POC notifies the CORHIO Service Desk within 24 hours and reference the CORHIO Sanctions for Participant Systems Misuse and CORHIO Sanctions for Unauthorized Use or Disclosure of PHI for the necessary disciplinary actions. If the Participant and CORHIO decide to blacklist the User from the HIE system, reference the process described above.

Within 72 hours: If the change is unrelated to non-compliance with CORHIO policies, the Participant POC shall notify the CORHIO Service Desk within *72 hours*.

If a Participant needs to deactivate all organization users, the CORHIO Service Desk may lock out the organization.

The CORHIO Service Desk will be available to assist the Participant POC in deactivating Authorized Users. Prior to contacting the Service Desk, the Participant POC shall complete the Participant's Deactivation User Request Form with the proper user information prior to contacting the CORHIO Service Desk.

MAINTAINING AUTHORIZED USERS LIST

The CORHIO Service Desk will use reasonable efforts to maintain a current status of Authorized Users using HIE tools and reports. Participant POCs may request the CORHIO Service Desk to run reports on the Participant's Authorized Users in the HIE system.

APPENDIX C - PatientCare 360 User Roles Definitions

ER Provider (does not have to select "Access Additional Records" in PatientCare 360)

- Physician, Physician Assistant, or Nurse Practitioner
- Access to all patients within PatientCare 360 without having to "access additional records"
- Access to all data sources and data (except in CERT)

Provider (can "access additional records" in PatientCare 360)

- Physician, Physician Assistant, Nurse Practitioner, PhD, PsyD, DDS, DOM, DPM
- Access to all patients within the HIE that a provider in their organization has a relationship with
- Access to all data sources and data types (within relationships)
- Can "access additional records" in PatientCare 360 and enter reason to get access to patients and patient data where a relationship is not currently established
- No VIP in PatientCare 360
- No Confidential in PatientCare 360

Billing Staff (cannot "access additional records" in PatientCare 360)

- Staff supporting one or more Physicians, Physician Assistants, or Nurse Practitioners
- Access to all patients within the HIE that a provider in their organization has a relationship with
- Access only to patient face sheets in PatientCare 360°™ for billing purposes. No access to clinical results.
- Can't "access additional records" in PatientCare 360°™ to view patients outside of an established relationship
- No VIP in PatientCare 360°™
- No Confidential in PatientCare 360°™

Staff (can "access additional records")

- Staff supporting one or more Physicians or Nurse Practitioners
- Access to all patients within the HIE that a provider in their organization has a relationship with
- Access to all data sources and data types (within relationships)
- Can "access additional recods" and enter reason to get access to patients and patient data where a relationship is not currently established
- No VIP
- No Confidential

Staff (cannot "access additional records" in PatientCare 360)

- Staff supporting one or more Physicians, Physician Assistant, or Nurse Practitioners which require
- a lower level of access
- Access to all patients within the HIE that a provider in their organization has a relationship with
- Access to all data sources and data types (within relationships)
- Can't "access additional records" in PatientCare 360 to view patients outside of an established relationship
- No VIP in PatientCare 360
- No Confidential in PatientCare 360

Quality Assurance (QA) Tester without "access additional records" (does not have to select "access additional records" in PatientCare 360)

- Assigned to testers performing QA
- Access to all patients without having to select "access additional records" in PatientCare 360
- Access to all data sources and data
- No VIP in PatientCare 360 unless necessary for testing
- No Confidential in PatientCare 360 unless necessary for testing

QA Tester with "access additional records" (can "access additional records" in PatientCare 360)

- Assigned to testers performing QA
- Access to all patients within the HIE that a provider in their organization has a relationship with
- Access to all data sources and data types (within relationships)
- Can "access additional records" in PatientCare 360 and enter reason to get access to patients and patient data where a relationship is not currently
- No VIP in PatientCare 360 unless necessary for testing
- No Confidential in PatientCare 360 unless necessary for testing

Quality Measure

- Assigned to individuals responsible for performing Medicare/Medicaid Quality Measures
- Access to designated patients without having to "access additional records" in PatientCare 360
- Access to designated data sources and data
- No VIP in PatientCare 360 unless necessary for reporting
- No Confidential in PatientCare 360 unless necessary for reporting

"Access Additional Records" Reasons

- New Patient
- Referred Patient
- Transferred Patient
- Additional Information Needed on Existing Patient
- Providing Coverage for Another Physician's Patient
- Information Needed for Billing
- Patient Presented for Emergency Care
- Quality Assurance

APPENDIX D - Provider Role Definitions

- **Part-time Office Based Provider:** A provider who works on average less than 25 hours per week during the month
- **Full-time Office Based Provider**: A provider who works on average 25 hours or more per week during the month
- **Volunteer Office Based Provider**: A provider who does not receive any financial or other non-financial compensation from Participant or any other entity for the services provided on behalf of Participant.

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
Dec-10	1	Melissa Erikson	Initial publication
Mar-11	1.1	Rebecca Rainey	Updated required fields for adding new users
May-11	1.2	Rebecca Rainey	Updated process for adding new authorized users to production if they are already active certification environment users – no additional forms will need to be submitted for production, a Service Desk ticket indicating which CERT users must migrate to PROD
Jul-11	1.3	Rebecca Rainey	Added PatientCare 360 User Roles Description Appendix
Sept-11	1.4	Rebecca Rainey	Added Appendix B for Provider Role Definitions
Oct-11	1.5	Rebecca Rainey	Updated PatientCare 360 User Roles Description Appendix
Apr-12	1.6	Janeece Lawrence	Modified to better reflect the role of CORHIO's Security Response Team
Dec-12	1.7	Janeece Lawrence	Revised to define "users, providers, and systems"
July-6	1.8	Janeece Lawrence	Changed name from break glass to access additional records

SECURITY PROTOCOLS

Procedure: CORHIO Security Plan and Procedure – Safeguards

PURPOSE

To define and identify the administrative, physical, and technical system safeguards to prevent unauthorized access and protect PHI.

SCOPE

Security Plan and Procedures: Procedures and specifications for administrative, physical, and technical safeguard

POLICY

Protect PHI obtained from the contributing Participants by establishing appropriate administrative, physical, and technical safeguards, including mechanisms for authorizing, granting, removing, and reporting user access (See User Authorization Policy);

CORHIO shall protect the Patient Information stored in accordance with the CORHIO Policies and Laws (See Security Protocols Policy). The MPI may be queried by Authorized Users, utilizing search elements specified in the CORHIO Procedures, as a means to access Patient Records residing with other Participants, and may be used only for permissible purposes as defined by CORHIO (See Appropriate Use and Disclosure Policy).

When searching the MPI, Authorized Users must provide, at a minimum, the mandatory data fields, as required by the CORHIO Procedures.

CORHIO, its System Providers, and Participants shall use, at a minimum, generally accepted administrative, physical, and technical security safeguards and processes to secure PHI as defined by applicable Laws, including HIPAA and HITECH.

CORHIO shall establish an appropriate and generally accepted level of security controls, including administrative, physical, and technical safeguards, by employing industry standard security technologies and processes.

PROCEDURE

Administrative Controls

- CORHIO implementation staff will work with the Participant and designated POC to collect appropriate user information to establish user connection to the HIE. The Participant will need to complete a CORHIO User Request Form, including the user's manager's signature, for each new user. CORHIO will store an electronic copy of the User Request Form for auditing purposes.

- Only those CORHIO and Medicity personnel explicitly authorized by the CORHIO Security Officer shall be granted access to the data center and/or the cages within the data center.
- Only CORHIO and Medicity personnel with a reasonable need shall be authorized to enter the data center and cages within the data center.
- CORHIO's Security Officer shall maintain the official list of explicitly authorized personnel.
    - Immediately upon termination or change of duties, the Security Officer shall remove said personnel from all access lists pertaining to patient data.
    - The designated Security Officer shall receive regular reports detailing user access (entry and exit) to the data center and cages within.

Physical Controls

- All patient health data shall reside on servers within a HIPAA/HITECH certified data center utilizing locked cages.
- Only those personnel explicitly authorized by the CORHIO Security Officer shall be granted entry to the data center and cages within the data center.

Technical Controls

- No patient data in the HIE shall reside outside the servers in the data center.
- Remote access shall be granted to only those authorized by the CORHIO Security Officer.

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
12/8/2010	1	Kurt Schmeer	Original Document
3/29/2012	1.1	Kelly Joines	Updated to clarify participant Point of Contact (POC) role

Procedure: Designate Security Response Team

PURPOSE

To define and identify the method by which a security response team is chosen/identified, including the Security Officer, Privacy Officer and Compliance Officer. This document will also identify the Security Response Team officials as well as their applicable backups. Also included, are the specific responsibilities for each Security Officer.

SCOPE

Security Plan and Procedures: Designate a Security Response Team

POLICY

In accordance with the HIPAA Rules, CORHIO shall designate officials responsible for security matters (e.g. Information Security Officer).

PROCEDURE

The Executive Officer, with input from the CORHIO leadership team, shall designate a Security Response Team, to include a Security Officer, Privacy Officer and Compliance Officer. The Security Officials shall have an unlimited term. Upon termination for any reason, the Chief Executive Officer shall propose and designate a replacement for any applicable Security Official as soon as is reasonably possible.

POSITION AND ROLES

The **Security Officer** oversees all ongoing activities related to development, implementation, maintenance of, and adherence to CORHIO policies and procedures covering security of and access to PHI in compliance to federal and state laws and health system security practices. The Security Officer ensures that periodic risk assessments and ongoing monitoring of key elements of the security program are completed.

RESPONSIBILITIES:

- Leads in the development and enforcement of information security policies and procedures, measures and mechanisms to ensure the prevention, detection, containment, and correction of security incidents
- Ensures that security standards comply with statutory and regulatory requirements regarding health information
- Ensures that security policies are maintained that include administrative security, personnel security, physical safeguards, technical security, and transmission security
- Assures appropriate documentation of response of the institution to the addressable portions of the security rule
- Ensures that security procedures are maintained that include evaluation of compliance with security measures; contingency plans for emergencies and disaster recovery; security incident

response process and protocols; testing of security procedures, measures, and mechanisms, and continuous improvement; and security incident reporting mechanisms and sanction policy

- Ensures that appropriate security measures and mechanisms are in place to guard against unauthorized access to electronically stored and/or transmitted patient data and protect against reasonably anticipated threats and hazards, including, when appropriate: integrity controls, authentication controls, access controls, encryption, abnormal condition alarms, audit trails, entity authentication, and event reporting
- Oversees on going security monitoring of CORHIO information systems, including periodic information security risk assessments, functionality and gap analyses to determine the extent to which key business areas and infrastructure comply with statutory and regulatory requirements, and review of new information security technologies and counter-measures against threats to information or privacy
- In coordination with the CORHIO Privacy Officer, oversees training programs, periodic security awareness reminders, and periodic security audits
- Serves as the CORHIO resource regarding matters of informational security
- Cooperates with CMS, other legal entities, and organization officers in any compliance reviews or investigations
- Coordinates with appropriate CORHIO Workforce Members and Participating Organizations to ensure timely development and implementation of corrective action plans in response to monitoring deficiencies and complaints
- Additional duties as assigned

The **Privacy Officer** oversees all ongoing activities related to development, implementation, maintenance of, and adherence to CORHIO policies and procedures covering privacy of and access to PHI in compliance with federal and state laws and health system privacy practices.

The Privacy Officer ensures that periodic risk assessments and ongoing monitoring of key elements of the privacy program are monitored.

RESPONSIBILITIES:

- Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures
- Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with CORHIO's Security Officer
- Works with legal counsel and leadership to ensure that CORHIO has and provides appropriate privacy and confidentiality documentation, authorization forms, and information notices and materials reflecting current legal practices and requirements
- Oversees, directs, delivers, and ensures delivery of initial privacy training and orientation to all workforce members
- Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all patient complaints concerning the organization's privacy policies and

procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel
- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, and extended workforce in cooperation with leadership and legal counsel as applicable
- Initiates, facilitates, and promotes activities to foster information privacy awareness within CORHIO and participating organizations
- Reviews all system-related information security plans to ensure alignment between security and privacy practices, and acts as a liaison to IT
- Works with all organization personnel involved with any aspect of protected health information to ensure full coordination and cooperation under the organization's policies and procedures and legal requirements
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance
- Serves as information privacy consultant to Participating Organizations as appropriate
- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations
- Coordinates the appropriate CORHIO workforce to ensure timely development and implementation of corrective action plans in response to monitoring deficiencies and complaints

The **Compliance Officer** oversees the overall HIE Privacy and Security Program, functioning as an objective body that reviews and evaluates compliance issues/concerns within the organization. The position ensures the Board of Directors, management, and employees are in compliance with the rules and regulations of regulatory agencies, the company policies and procedures are being followed, and that behavior in the organization meets the company's standards of conduct.

RESPONSIBILITIES:

- Develops and periodically reviews and updates Standards of Conduct to ensure continuing currency and relevance in providing guidance to management and employees
- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations
- Consults with the corporate attorney as needed to resolve difficult legal compliance issues.
- Acts as an independent review and evaluation body to ensure that compliance issues/concerns within the organization are being appropriately evaluated, investigated, and resolved
- Ensures proper reporting of violations or potential violations to duly authorized enforcement agencies as appropriate and/or required
- Monitors the performance of the Privacy and Security program and relates activities on a continuing basis, taking appropriate steps to improve its effectiveness

SECURITY RESPONSE TEAM:

Compliance Officer – Brian Braun

Backup – Kelly Joines

Privacy Officer – Robert Denson

Backup – TBD (Policy Director)

Security Officer – Jose Seto

Backup – RJ Gomez

REVISION HISTORY

REVISION DATE	REVISION OWNER	COMMENTS
6/23/2010	Tony Gregorio	
9/26/2011	Terri Skalabrin	Updated to remove references to CIO
1/29/2013	Robert Denson	Updated to add Compliance and Privacy Officer and removed Executive Director. Added SRT current staff/backups and responsibilities.

Procedure: CORHIO Security Event Investigation and Breach Notification to Participant Organizations

PURPOSE

As required by the Security and Privacy provisions of HIPAA and HITECH, Participants and Business Associates must follow specific steps to respond to ***any breach of unsecured PHI.***

These requirements apply if all of the following are present:

- There is a "breach." The Rule defines "breach to mean the unauthorized acquisition, access, use or disclosure of PHI."
- The PHI is "unsecured." The Rule defines unsecured PHI to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption and destruction as specified by Department of Health and Human Services (HHS) guidance.
- The breach "compromises the security of the PHI." Under the Rule, this occurs when there is a significant risk of financial, reputational, or other harm to the individual who's PHI has been compromised.

As a Business Associate, CORHIO will maintain a Breach Response Plan outlining the appropriate response and notification process to be followed in the event of a breach of unsecured PHI. The plan includes the following components:

- **Security Response Team:** Workforce members and responsibilities for security event investigation, communication and breach notification
- **Risk Assessment**: Risk analysis steps in the event of a breach

Breach Notification: Response and notification requirements in the event of a breach

SCOPE

This procedure applies to all CORHIO Workforce Members and Participant Organizations.

PROCEDURE

Risk Assessment and Analysis

- A risk assessment and investigation and will be conducted by the CORHIO Security Response Team in the case of a security event. The assessment will evaluate the following factors:
    - **Nature and extent of PHI involved**: Analysis of the type of PHI involved will be conducted to determine the likelihood that the PHI could be used by an unauthorized recipient to further its own interests. For example; the nature of services as well as the amount of detailed involved (i.e., treatment plan, diagnosis, medication, medical history information, and test results) should be considered.
    - **Likelihood that the information is accessible and usable**: An assessment regarding whether the unsecured PHI will be or has been used by an unauthorized individual(s).

- **Unauthorized person who impermissibly used or received PHI**: Identification of the person(s) who impermissibly used or received PHI and whether the recipient is otherwise obligated to protect the privacy and security of PHI (such as medical practice or other HIPAA covered entity). If the information impermissibly used or disclosed is not immediately identifiable. CORHIO will determine whether the unauthorized person who received PHI has the ability to re-identify the information.
- **Whether the PHI was actually acquired or viewed**: CORHIO will distinguish uses or disclosures where PHI was actually compromised from those that merely involved the potential for improper access to PHI.
- **Extent to which the risk of the breach has been mitigated:** CORHIO will consider the extent and efficacy of any mitigation steps that have been taken.
- **The risk analysis will identify the breach prevention, ongoing monitoring, auditing and other mitigation measures CORHIO will take in response to the breach**

- Ongoing Risk analysis will continually monitor the three types of security safeguard required by the HIPAA Security Rule listed below to evaluate and continually mitigate any vulnerability.
  - **Administrative**
    - Procedures and demonstration of a risk management process
    - Policies and procedures relevant to operational security
    - Information access restriction requirements and controls
    - Incident response procedures and disaster recovery plans
    - Evidence of periodic technical and non-technical reviews
  - **Physical**
    - Physical access controls (such as data center access and appropriate record keeping
    - Policies and procedures for workstation security
    - Proper usage, storage, and disposal of data storage devices
  - **Technical**
    - Auditing and audit procedures
    - Use of encryption devices and tools
    - Implementation of technology to ensure PHI confidentiality, integrity and availability

SECURITY RESPONSE TEAM AND RESPONSIBILITIES

CORHIO will maintain a Security Response Team comprised of the following CORHIO Workforce Members:

- Privacy Officer
- Security Officer
- Compliance Officer

Members of the Security Response Team will maintain awareness of the current and evolving federal and state laws applicable to breach notification, reporting and disclosure.

Any Workforce member may report a suspected breach to either the CORHIO Help Desk or Security Response Team.

Any member of the Security Response Team is authorized to trigger a security event investigation.

The Privacy Officer will serve as the communications coordinator and the single point of contact between CORHIO and Participating Organizations.

The Security Officer will ensure that the Privacy Officer has a clear understanding of the technical details pertaining to a breach to ensure that external communication is appropriate, timely and accurate.

SECURITY EVENT INVESTIGATION

A security event which is deemed a breach of PHI shall be treated as "discovered" as of the first day on which the breach is known to CORHIO.

If a security event or possible breach of unsecured protected health information occurs at or by CORHIO, the Privacy Officer will be responsible for the management of the security event investigation, completion of the risk assessment, and working in coordination with the members of the Security Response Team.

RISK ASSESSMENT

For acquisition, access, use, or disclosure of PHI to constitute a breach, it must be in violation of the Privacy Rule. The risk assessment conducted in the event of a breach will:

- **Determine whether the use of disclosure of PHI is in violation of the HIPAA Privacy Rule:** For acquisition, access, use, or disclosure of PHI to constitute a breach it must constitute a violation of the HIPAA Privacy Rule. For example, if information is de-identified in accordance with 45CFR 164.514 (b), it is not PHI and any inadvertent or unauthorized use or disclosure of such information will not be considered a breach under the requirements of the rule.
- **Determine whether there is a use or disclosure that compromises the security and privacy of PHI:** HHS has clarified that a use or disclosure that "compromises the

security and privacy of PHI" means a use or disclose that "poses a significant risk of financial, reputational, or harm to the individual."

- **Assess whether any exceptions to the Breach Definition apply:** The Rule identifies exceptions to the definition of "breach" under the Act:
    - *The unintentional acquisition, access, or use of PHI by any Workforce Member or person acting under the authority of a Participant or business association if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in future use or disclosure in a manner not permitted by the Privacy Rule*
    - *The inadvertent disclose of PHI by an individual otherwise authorized to access PHI at a facility operated by a participant or business associate to another person of same covered entity or business associate*
    - *An unauthorized disclosure where a Participant or business associate has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information*

- The breach investigation and risk assessment documentation will address:
    - Consideration of who impermissibly used or to whom the information was impermissibly used
    - The type and amount of PHI involved
    - The potential for significant risk of financial, reputational, or other harm
    - If a determination is made that an exception to the rule applied; why that determination was made and why the impermissible use or disclosure fell under one of the exceptions

PARTICIPANT ORGANIZATION BREACHES

If a general breach or suspected breach occurs at or by a Participant Organization involving CORHIO, the Participant Organization will:

- Provide notice to CORHIO within 24 hours of discovery
- Conduct a security event investigation and risk assessment
- Provide the CORHIO Privacy Officer with the findings as outlined in the CORHIO Investigation and risk assessment process

Following the discovery of a breach specific to unsecured PHI by or at a Participant Organization involving CORHIO, the POC will:

- Provide notice to CORHIO no later than 14 days from the discovery of the breach
- Conduct and fully document an investigation of the breach
- Provide CORHIO with:
    - The identification of each individual whose unsecured protected health information has been, or is reasonably belief to have been, accessed, acquired, or disclosed
    - Any other available information that the Participant Organization is required to include in notification to individuals

NOTIFICATION

Following the discovery of a breach of unsecured PHI, CORHIO will immediately notify the appropriate
Participant Privacy, Security or Compliance Officers so that the Participant can, in turn, notify the affected individuals as required by the Security Rule.

- CORHIO will provide notice to the Participant no later than 14 days from the discovery of the breach
- CORHIO will conduct and fully document an investigation of the breach
- The Privacy Officer will provide the Participant with:
  - The identification of each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed acquired or disclosed
  - Any other available information that the Participant Organization is required to include in notification to individual(s)

In addition, CORHIO will follow the HIPAA requirements for further notification, and under the DURSA, as soon as reasonably practicable, but no later than 24 hours after determining that a breach has occurred, CORHIO shall provide a notification to all Participants likely impacted by the breach and the Coordinating Committee of such breach.

RISK MITIGATION

The CORHIO Security Response Team will immediately review the results of all breach investigations to ensure that risks and vulnerabilities identified through the investigative process are appropriately evaluated and mitigated.

WORKFORCE TRAINING

All CORHIO Workforce Members will be trained on the Breach Investigation and Notification to Participant Organization procedures. Workforce Members will also be provided training regarding how to identify potential breaches as a component of CORHIO's ongoing risk assessment program.

SANCTIONS

CORHIO will maintain and apply appropriate sanctions against Workforce members who fail to comply with Privacy and Security policies and procedures.

DOCUMENTATION

All breach investigations will be documented and maintained by the Privacy Officer for a period of no less than six 6 years.

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
July-10	V1.0		Initial publication
June-13	V1.1	Kelly Joines	Included HIPAA final rule on changes to breach policy
February-14	V1.2	Robert Denson	SRT Review

ACCESS AND DISCLOSURE AUDITING

Procedure: CORHIO Disclosure Accounting Procedures

DEFINITIONS

Electronic Health Record (EHR): An EHR system is designed to store organize and provide access to EHR records electronically on a computer. This document uses the term EHR when referencing the EHR systems used by participants in their facilities.

Health Information Exchange (HIE): HIE is defined as the mobilization of healthcare information electronically across organizations within a region, community or hospital system.

Master Patient Index (MPI): Master Patient Index (MPI) is a database that maintains a unique index (or identifier) for every patient registered at a health care organization (HCO). The MPI is used by each registration application (or process) within the HCO to ensure a patient is logically represented only once and with the same set of registration demographic/registration data in all systems and at an organizational level. It can be used as enterprise tool to assure that vital clinical and demographic information can be cross-referenced between different facilities in a health care system. An MPI correlates and cross-references patient identifiers and performs a matching function with high accuracy in an unattended mode. An MPI is considered an important resource in a healthcare facility because it is the link tracking patient, person, or member activity within an organization (or enterprise) and across patient care settings.

Participant: The Participant is the organization that has subscribed to CORHIO services.

Point of Contact (POC): A Point of Contact is designated for each Participant organization and is authorized to provide CORHIO with end user updates (add, change, deactivate) and to request services such as audits from CORHIO.

Protected Health Information (PHI): PHI under HIPAA includes any *individually identifiable* health information. *Identifiable* refers not only to data that is explicitly linked to a particular individual (that's *identified* information). It also includes health information with data items which reasonably could be expected to allow individual identification.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Site Administrators: Participant Site Administrators are granted privileges in the HIE system that provide the capability to run predefined audit reports and establish or modify other site settings as outlined in the Site Administrator training.

Disclosure Accounting Principles

PURPOSE

This document defines the procedures to obtain a disclosure report from the HIE System or request a disclosure report from the CORHIO Service Desk. Also defined is the record retention information for the HIE system logs.

SCOPE

This document is for Participants and CORHIO staff.

HIE SYSTEM LOG

The HIE system maintains a log that records a variety of information regarding the users, transactions, and system activities. The log is used to create reports for audit purposes. The system reports are accessible by the CORHIO System Administrator(s) and participant site administrators.

PREDEFINED DISCLOSURE REPORTS

The current list of predefined disclosure reports is provided below. Typical disclosure audits use the following reports: Patient Chart Access by Patient, Patient Chart Access by User, and Organization Break Glass Audit Log.

USER LOGIN HISTORY

Report Name	Description
User Login History By Org	Returns login history for all users in the specified organization
User Login History By User	Returns login history for the specified user
Active Users	Lists the number of active users in the specified organization(s)

PHYSICIAN LOGIN

Physician Login Summary	Annual summary of the logins for all physicians in a single repository

Patient Chart Access

Patient Chart Access By Org	Patient chart access for all users in the specified organization
Patient Chart Access By Patient	Patient chart access for the specified patient
Patient Chart Access By User	Patient chart access for the specified user

CLINICAL INBOX ACTIVITY

Clinical Inbox Activity By Org	Summarizes Clinical Inbox actions taken by users in the specified organization(s)
Clinical Inbox Activity By Patient	Summarizes which users have taken action on a specified patient's information from Clinical Inbox
Clinical Inbox Activity By User	Summarizes which patients have had Clinical Inbox actions taken by the specified user

BREAK GLASS AUDIT LOG

Organization Break Glass Audit Log	Break Glass Audit Log (Long and Short Term) for all the users in the specified organization
User Break Glass Audit Log	Break Glass Audit Log (Long and Short Term) for the specified user
Patient Break Glass Audit Log	Break Glass Audit Log (Long and Short Term) for the specified patient
Who Broke Glass to see my Patients	Who Broke Glass (Long and Short Term) to see Patients of specified provider

Patient Merge CDR Reports

Patient Merge/Link By User	Returns merge and link details by user
Encounter Move Detail By User	Returns encounter move details by user
Manual CDR Action Summary	Returns encounter and identifier moves, links, merges and differentiations summary

PATIENT MOVE/LINK MPI REPORTS

Patient Move-Link MPI Reports	Returns move and link details by user
Manual MPI Action Summary	Returns patient moves and links summary

DELIVERY REPORT

Delivery Report By Org	Identifies the delivery method and location for each result for the specified organization(s)
Delivery Report By Patient	Identifies the delivery method and location for each result for a specified patient. Information is available for the current and previous month

COMMUNITY DOCUMENT ACTIVITY

CCD Activity By Org	Summarizes CCD actions taken by users in the specified organization(s)
CCD Activity By User	Summarizes which patients have had CCD actions taken by the specified user
CCD Activity By Patient	Summarizes which users have taken action on the specified patient's information using CCDs

Medication History Queries

Medication History Queries By Org	Summarizes Medication History Queries initiated by users in the specified organization(s)
Medication History Queries By User	Summarizes Medication History Queries initiated by specified user
Medication History Queries By Patient	Summarizes which users have initiated Medication History Queries on a specified patient

GENERATING OR REQUESTING A DISCLOSURE ACCOUNTING REPORT

Administrators at each participant site have the ability to run predefined reports of system usage and data disclosures. Site administrators are trained to run the reports during HIE system training. End users may contact their administrator or their designated HIE Point-of-Contact (POC) to request an audit. The POC can request the audit from the local administrator or from CORHIO.

Administrators will run the requested audit and provide the results to the requester directly. Audits can be requested through CORHIO by the POC by opening a service request with the HIE Service Desk. Audits provided by CORHIO will be delivered to the POC and the participant organization will deliver the results to the requester.

Contacting the CORHIO Service Desk

A service request can be opened using the following methods:

Phone	1-877-MY1-CORHIO	Outside Denver Metro
	1-877-691-2674	
	720-285-3277	Denver Metro
Web Desk	https://helpdesk.corhio.org/logins/corhiologin.htm	
Email	helpdesk@corhio.org	
Pager	For critical support options Available via the Web Desk or Phone support	

SERVICE REQUEST RESPONSE TIME

The expected response time for audit/report requests will follow the HIE Service Desk response goals.

Request Type	Time to Respond Goal
Phone Calls	The Service Desk will respond to voice mail messages within 2 hours for messages left on the Service Desk phone line. For critical requests, customers and employees should follow prompts for critical support.
Service Request Tickets	The Service Desk will respond to tickets, opened via the web desk or email requests sent to helpdesk@corhio.org, within 2 hours if the request is received during business hours, Monday through Friday. Responses to e-mails or tickets received after 5:00PM MT will be handled by 10:00AM the next business day. Critical requests should be opened using the ticket system or by following the phone prompts for critical support.

Critical Service Request Tickets	The Service Desk will respond to pager notifications for critical support within 30 minutes of receipt of the page.

Revision History

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
12/8/2010	1.0	Susan Clark	Original Document
3/1/2011	1.1	Patty Cerna	Updated to include available Medicity reports
4/21/2011	2.0	Patty Cerna	Updated with final service desk contact information.
3/29/2012	2.1	Kelly Joines	Updated to remove indication that participants are able to perform user maintenance activities within PatientCare 360.

Procedure: CORHIO Inappropriate Use and Non-Compliance Reporting Procedure

PURPOSE

The purpose of this document is to define the procedures for participants to effectively report potential inappropriate HIE system use or non-compliance with CORHIO's policies.

SCOPE

This document is for Participants and CORHIO staff.

POLICY

CORHIO has a strict policy for inappropriate use of the CORHIO system or non-compliance with CORHIO's Appropriate Use of Services policies.

The terms "inappropriate use" and "non-compliance" refer to users with access to PHI using, disclosing, or requesting it in a manner not permitted by CORHIO policies.

Authorized users who violate CORHIO Policies shall have their user account disabled and system access denied, immediately, and the Participant shall be notified so that disciplinary action can be pursued in accordance with the Participant's own internal policies.

Inappropriate use and non-compliance can be discovered and reported either by CORHIO in its audit processes or by Participants.

CORHIO reserves the right, at its sole discretion, to temporarily or permanently deny access to users suspected of inappropriate use and/or non-compliance. Permanent denial of access is termed blacklisting.

PROCEDURE

Reporting of Potential Inappropriate Use or Non-Compliance to CORHIO by a Participant
If an authorized user has been disciplined for using, disclosing, or requesting PHI in a manner not permitted by CORHIO policies, the disciplining/managing Participant shall notify CORHIO's Service Desk immediately for further investigation, and submit a User Access Change Form within 72 business hours, indicating that the disciplined user shall be permanently blocked from the system for inappropriate use or non-compliance.

Upon receipt of the User Access Change form, CORHIO's Operations organization shall immediately exclude the user from access to the CORHIO system and indicate that the exclusion is permanent and the user has been blacklisted.

Reporting of Potential Inappropriate User or Non-Compliance by CORHIO
CORHIO will regularly audit the system to ensure appropriate use by Participants and authorized users. If, during the course of audit activities, CORHIO discovers suspect behavior for a given user, CORHIO may immediately suspend the user account as part of its investigative activities.

CORHIO's Security Response Team (SRT) will notify the escalation resource within the Participant organization of the account suspension and investigation activities immediately upon discovery. Working with the Participant escalation resource, the SRT will investigate the potential inappropriate use and/or non-compliance activities and determine if the user must be subsequently permanently denied access to the system.

If CORHIO discovers inappropriate use and/or non-compliance activities and has not already suspended the user's account, CORHIO shall immediately exclude the user from access to the CORHIO system and may indicate that the exclusion is permanent. If the account is already suspended, CORHIO may update the suspension to a permanent exclusion.

CORHIO will provide written notification to the Participant escalation resource of the final disposition of the investigation within 72 hours so that disciplinary action in accordance with the Participant's own internal policies can be pursued if necessary.

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
12/8/2010	1	Susan Clark	Original Document
3/29/2012	1.1	Kelly Joines	Clarified permanent exclusion/blacklisting and modified Security Officer activities to Security Response Team (SRT) activities.

Procedure: CORHIO System Usage – Access Auditing Procedures

PURPOSE

This document defines the procedures to identify security relevant events and the data to be collected and communicated as determined by CORHIO's Governing Principles and Policies.

SCOPE

This document is for Participants and CORHIO staff.

POLICY

The CORHIO PatientCare 360 application shall include an audit log documenting which Authorized Users or Data Providers have taken any actions to post, modify, access, or otherwise interact with information about patients, including data regarding the action(s) taken. Audit log information is available to Participants.

CORHIO shall conduct periodic audits in compliance with its Access and Disclosure Auditing Policy to assure the adequacy of the Master Patient Index and its algorithms.

PROCEDURE

System Audit

The PatientCare 360 Audit Trail enabling service generates a record of the users who have accessed which files and when. The enabling service also makes note of any attempts to access the system from an unauthorized terminal, the use of an expired username or password, unusual numbers of password attempts, and other potential attempted violations of security policies.

An audit is kept of every transaction in PatientCare 360. The audit process documents every step in the information exchange process, whether the transaction is discarded (because the receiver did not want the information), who it was sent to, when it was sent and received, what happened to the data upon receipt (examples: printed, viewed, or acknowledged by an EHR interface). The original message as it was received, along with the message as it was transformed for delivery to the practice (such as to an EHR) is kept in the audit. This information is available to the CORHIO administrative user(s) as well as to each participant that received the message.

A record shall be maintained that records all assigning of access permissions as well as updates and deactivations.

All security vulnerabilities are reviewed by both the CORHIO Security Response Team and CORHIO's vendor, Medicity. Based on these reviews, CORHIO and Medicity will mutually identify which vulnerabilities require remediation or correction. Medicity will then remediate or correct those vulnerabilities identified as directed by and agreed with CORHIO. Medicity will provide evidence of completion of each task, subject to verification by CORHIO.

PARTICIPANT AUDIT

Any access to the PatientCare 360 system is logged and can be viewed online by CORHIO and participant administrator(s). CORHIO authorized administrative users can view any audit trail information throughout the system. Participant administrators can view audit trails pertaining to the staff users that work on their behalf in their practice office.

Suspicious accesses will trigger warning messages that will be sent to the CORHIO SRT team. The SRT Team will determine if an involved participant shall be notified of the suspicious access.

All access to all PHI and ePHI is logged. Audit records and access logs shall retain the following information:

- Date and time of user access/action
- User ID and name
- Successful and unsuccessful login attempts
- Logging out
- Source institution of an access request, if available
- IP Address of user (if web access)
- Web browser of user (if web access)
- URL accessed (if web access)
- Type and content of data accessed and actions/activities performed by the user including:
    - Selecting a patient from the search results for the purpose of viewing clinical data
    - Viewing clinical results categories for a specific patient
    - Patient identifier such that the patient can be positively identified regardless of at what point in time the patient's data was accessed
- Medical record number
- Event types
- Data types
- Data identifiers

RANDOM AUDITS

All audits are performed continuously for all participants; therefore random audits are not necessary. However, review of specific, but randomly chosen participants shall be performed on a monthly basis equivalent to 5% of enabled active participants. A log listing random reviews and the results shall be maintained by CORHIO. Detection of suspicious activity will be reviewed by the CORHIO SRT Team. This team will determine if an involved participant shall be notified of the suspicious access.

ANNUAL SUMMARY REPORTS

Annual summary reports listing users, number of logins per user, date and time of first access per user, and date and time of last access per user for each participant may be requested by each participant organization. Annual summary reports of system audits shall be compiled and may be published on the CORHIO website.

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
12/8/2010	1	Patty Cerna	Original Document
3/29/2012	1.1	Kelly Joines	Modified to reflect CORHIO's SRT and PatientCare 360.

SYSTEMS MANAGEMENT

CORHIO HIE System Maintenance and Support Agreement

HIE System Maintenance and Support Services

HIE software maintenance and support is available through CORHIO to all HIE subscription users as part of the Participant Agreement. The HIE system is provided to CORHIO and its end users as Software as a Service (SaaS).

CORHIO offers the following software maintenance and support functions:

- Issue resolution activity Monday – Friday, 8 am – 5 pm, excluding holidays, for all non-critical priority issues reported to CORHIO
- 24x7 issue resolution activity on critical priority issues
- Onsite assistance as deemed necessary by CORHIO and Participant
- All "point releases" for the HIE software
- All "patch releases" for the HIE software
- Initial monitoring and assisting Participants with correcting batch job failures
- Initial monitoring and assisting Participants in managing CORHIO interface engine message queues: finding and processing failed/stuck messages

Holidays excluded from non-critical issue resolution activity include: New Year's Day, Martin Luther King, Jr. Day, President's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, the Friday following Thanksgiving, Christmas Eve, and Christmas Day.

Critical Priority	Patient safety and/or CORHIO, participant or user business integrity or continuity are in jeopardy. Loss of Service, or serious impairment of Service has occurred or is reasonably likely to occur, which loss or impairment cannot be reasonably circumvented. By way of example and not limitation: • Security Breach • Patient data is inaccurate or displaying incorrectly • Web server not accepting connections due to functionality or performance issues of Hosted System • Persistent inability to access clinical information due to functionality or performance issues of Hosted System • Critical feature of Hosted System does not work (identifiable part of functionality), no workaround exists or workarounds are impractical • Data is corrupted
High Priority	An issue or problem exists which can be reasonably circumvented or does not materially affect normal operations of the Hosted Systems. By way of example and not limitation: • A problem with a non-functioning feature of the Hosted System which is not critical to CORHIO or any participant or user exists (identifiable part of Hosted System functionality) • Part of a feature of the Hosted System is affected, and a viable workaround exists

	• Hosted System performance is less than optimum • Highly visible usability problem exists with the Hosted System, but does not affect functionality of the Hosted System • Participant or user issue with Hosted System response time • Failed Batch Processing job
Medium Priority	A non-critical process or functionality of the Hosted System is failing.
Low Priority	A situation where the Hosted System has complete functionality and is still accessible by CORHIO and the participants and users, but a bug exists.

Problem Reporting

All authorized users will be provided with instructions during training for contacting CORHIO's Service Desk for problem reporting. In general, a user will phone/email the CORHIO service desk to report problems or to make a support request and the service desk representative will require the following information to log a support ticket and troubleshoot the problem:

- User contact name
- User contact phone
- User contact email address
- User issue, request, or problem
- Detailed description of the problem
- Impact the problem is having on user's work activity

CORHIO will log a support ticket with the provided information, and assign and communicate a priority to the ticket. Priorities are defined as follows:

In many cases, since the system and its interface queues and batch jobs are being automatically monitored, CORHIO may report issues to participants before participants recognize the issue is occurring. CORHIO will work with the participating entity's single point of contact to communicate issues, issue status, and resolution.

Service Desk

The purpose of CORHIO's Service Desk is to provide first line support to HIE participant end users, addressing issues that fall into the scope of support, and escalating to HIE Software Vendor or CORHIO's Information Technology Staff.
In general, issues such as updating user account access, resetting passwords, addressing training and system functionality, and system audit requests will be resolved by the Service Desk.
Detailed information, ticket workflow, and help desk contact information will be provided to all end users during training activities.

Response Times

Response Type	Time to Respond Goal
Response to Phone Calls	The Service Desk will respond to voice mail messages **within 2 hours** for messages left on the Service Desk phone line. For critical requests, customers and employees should follow prompts for critical support.
Response to Service Request Tickets	The Service Desk will respond to tickets, opened via the web desk or e-mail requests sent to support@corhio.org, **within 2 hours** if the request is received during business hours, Monday through Friday. Responses to e-mails or tickets received after 5:00PM MT are made by 10:00AM the next business day. Critical requests should be opened using the ticket system or by following the phone prompts for critical support.
Response to Critical Service Request Tickets	The Service Desk will respond to pager notifications for critical support **within 30 minutes** of receipt of the page.
Notification of Planned HIE System Outages	The Service Desk will advise customers of planned outages **2 days prior** to the outage.
Notification of Unplanned HIE System Outages	The Service Desk will advise customers of unplanned outages **within 30 minutes** of confirmation of an outage.
Notification of Restoration of Services	The Service Desk will advise customers of the restoration of services **within 30 minutes** of advice or awareness that a service has been restored.

Message Delivery

Definition	Performance Expectation
Message means a message sent through the CORHIO System. Message Delivery Time means the time duration beginning from receipt of a Message by the	The CORHIO System will achieve a Message Delivery Time of 30 minutes or lower on at least 95% of the Messages sent during each month.

CORHIO System from a user and ending when the Message has been successfully delivered by the CORHIO System to the intended recipient. - The Message Delivery Times is calculated as the timestamp of the Message write at the edge server from which the Message is sent minus the timestamp of the Message delivery acknowledgement.	

System Maintenance Approach

SOFTWARE RELEASES

CORHIO Vendors periodically releases software upgrades throughout the year, of varying breadth. CORHIO expects to apply major and minor releases throughout the year and subsequently expects the participants to apply the releases as well. In general, CORHIO will be no more than two major release versions behind the current general release.
CORHIO and its Vendors, with input from participants, will evaluate the benefit of each release against the overall level of effort required for the upgrade and provide upgrade notification to participants at least two months in advance, unless otherwise negotiated with all participants.
Software is released into the live production system only after it has passed vendor quality assurance testing, CORHIO testing, and participant certification testing. Certification testing, or User Acceptance Testing, is done in a dedicated environment where all of the necessary interfaces are available to verify the changes in the software as well as regression test the environment.
Participant required level of effort for each User Acceptance Test for integrating new data types will be equal to or less than the level of effort outlined in the Participant Agreement for the initial installation. Not all releases will require participant testing, in which case participants will be notified of the upgrade so that they may report any subsequent issues, should they occur.
Participant required level of effort for each User Acceptance Test for planned software releases will vary from very little to approximately two weeks of new functionality and regression testing, depending on the magnitude and impact of upgrades. CORHIO will assign a project manager to work with each participant to plan out the appropriate and mutually-agreed upon level of testing and training required for each software release.
Once the software has been certified by participants, a production promotion date is agreed with Vendors and CORHIO and the participating entities are notified. CORHIO will work with all participating entities to address testing and scheduling of point and patch releases.

PLANNED DOWNTIMES

Planned downtimes will be communicated to all participating entities ahead of time via email notification from CORHIO to the designed participating entity single point of contact.

Maintenance & Support Limitations

Reported defects will generally be addressed as part of a scheduled maintenance release by severity on a first come, first served basis. Severe defects that fall outside of the scheduled maintenance release will be evaluated for correction on a case-by-case basis.

Updated to Maintenance & Support Procedures

These procedures will be evaluated on an ongoing basis and updated as needed. Participants will be notified of the updates as they are published.

Procedure: CORHIO Technical Security Specifications Management

The purpose of this document is to define the technical security specifications for participant implementation and secure data transmission with CORHIO.

SCOPE

This procedure applies to all HIE Participant Organizations.

POLICY

CORHIO shall provide technical security specifications to Participants as part of the implementation process. CORHIO will implement and maintain appropriate technical safeguards for the CORHIO System, including hardware and software protective mechanisms such as firewalls, intrusion detection, anti-virus, and protected networks (e.g. network infrastructure, remote access, and wireless networking controls). CORHIO and its system providers will utilize third-party audits and risk assessments on a schedule CORHIO deems appropriate.

Participants, and their system providers, shall conform to CORHIO's requirements for secure infrastructure and data transmission including appropriate hardware and software protective mechanisms such as firewalls, anti-virus, and protected networks (e.g. network infrastructure, remote access, and wireless networking controls).

Participants shall only allow Authorized Users to access the CORHIO system from secured end user environments.

System providers shall conform to CORHIO's requirements for secure infrastructure and data transmission including appropriate hardware and software protective mechanisms such as firewalls, antivirus, and protected networks (e.g. network infrastructure, remote access, and wireless networking controls).

System providers shall only allow system operations personnel and Authorized Users to access the CORHIO system and all its elements from secured end user environments.

PROCEDURE

CORHIO will provide minimum system requirements to each participant for maintaining the optimal usage of the PatientCare 360 application while offering standard security and virus protection for the personal computer connected to the application.

The following defines these minimum requirements:

- **Computer/Processor:** Intel or AMD processor(s) running at 2 GHz or faster – most processors made in the last two years are acceptable
- **Operating System**: Windows 7, Windows Vista, Windows XP, Windows Small Business Server 2003, or newer (with latest Service Packs), MAC OS

- **Browser**: Internet Explorer 7, 8, or 9 (compatibility mode is supported), Apple Safari v5 on MAC
- **Memory:** Windows XP Service Pack 2 (SP2) – 87 MB
  Windows XP Professional x64 Edition – 168 MB
  Windows Server 2003 Service Pack 1 (SP1) - 87 MB
  Windows Server 2003 Service Pack 1 ia64 – 218 MB
- **RAM**: 2 GB or more for local/client computers
- **Hard Drive**: At least 160 GB of free space
- **Connectivity**: An active high speed internet connection
- **Display**: Monitor with resolution 1 024 X 768 or higher
- **Adobe Reader** 6.0 or later
- **Adobe Flash** 8.0 or later

REVISION HISTORY

REVISION DATE	VERSION	REVISION OWNER	COMMENTS
3/1/2011	1	Kurt Schmeer	Original Document
1/17/2012	1.1	Rebecca Rainey	Updated Minimum Requirements based on updates from Medicity for IE 8 and 9
3/29/2012	1.2	Kelly Joines	Modified to include Adobe requirements, Mac OS, and Safari availability

Procedure: CORHIO Transition from Implementation to Support

PURPOSE

The purpose of this document is to outline the approach to transitioning a Participant from implementation to support.

SCOPE

This procedure applies to the Participant Organizations and CORHIO.

PROCEDURE

Prior to a Participant going live with HIE, CORHIO shall work with the Participant project team to establish escalation points and maintenance procedures post-live.

Prior to going live with the HIE, the CORHIO Project Manager will gather the necessary contacts for the Service Desk to effectively work with each Participant as they transition to maintenance. The goal of this information gathering is to establish clear Participant contacts and procedures for the CORHIO Service Desk to communicate both planned and unplanned activities. CORHIO will store the resulting Participant contacts and decision points as part of the Participant's organization record in the CORHIO Service Desk system. If a contact or procedure needs to be updated, it is the responsibility of the Participant's Point of Contact to submit a ticket to the CORHIO Service Desk or contact the Service Desk by phone to ensure that the Participant's maintenance contacts and procedures remain current.

In addition to gathering key contact information to provide to the Service Desk, the CORHIO Project Manager will share the communication plan the Participant must follow when any changes are made to their source system. Participants shall submit a service desk ticket whenever a change is made to their source system that may impact the HL7 messages coming into the HIE. The CORHIO team will determine if that change will require any processing changes by Medicity or any configuration changes by the Service Desk.

The following sections outline key contacts and data to be identified at each Participant location during the information gathering phase.

HOSPITALS AND DATA SENDERS

CORHIO will gather the appropriate Participant information and procedure requirements to facilitate the following CORHIO Service Desk communication points:

Facility Name	
Business Hours	
Security Officer	Name: Phone: Cell/Pager: Email Address:
Privacy Officer	Name: Phone: Cell/Pager: Email Address:
Compliance Officer (If Different)	Name: Phone: Cell/Pager: Email Address:
Contract Contact	Name: Phone: Cell/Pager: Email Address:

Communication Purpose	Description	Communication Contact Business Hours	Communication Contact Non-Business Hours
IT/Network Issues or Concerns	Procedure and Participant Contact for CORHIO Service Desk to contact if there is an issue with Nexus, the network, or other IT issues or concerns	Name: Phone: Email Address:	N/A
HIE System Upgrades	Procedures and Participant contact for CORHIO Service Desk to work with when the HIE is upgraded. HIE upgrades, including any planned downtime, are planned and communicated in advance	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
Critical Issues	Procedure and Participant contact for CORHIO Service Desk to contact if there are critical issues, including security events, unplanned downtime, patient safety issues, or other critical issues as defined in the Participant Agreement.	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
Opt In/Opt Out	Participant contact to confirm receipt of opt out/opt in requests and completion of opt out/opt in	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
Policy and Procedure Updates	Procedure and Participant contact for CORHIO Service Desk to contact with CORHIO Policy and Procedure updates	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
Participant System Upgrades	Procedure and Participant contact for CORHIO Service Desk to work with when Participant communicates an internal system upgrade or change that may impact HIE exchange	Name: Phone: Email Address:	N/A

PHYSICIAN PRACTICES AND DATA RECEIVERS

CORHIO will gather the appropriate Participant information and procedure requirements to facilitate the following CORHIO Service Desk communication points:

Facility Name	
Business Hours	
Security Officer/Compliance/Privacy Contact	Name: Phone: Cell/Pager: Email Address:

Communication Purpose	Description	Communication Contact Business Hours	Communication Contact Non-Business Hours
IT/Network Issues or Concerns	Procedure and Participant contact for CORHIO Service Desk to contact if there is an issue with Nexus, the Network, or other IT Issues or concerns	Name: Phone: Email Address:	N/A
Critical Issues	Procedure and Participant contact for CORHIO Service Desk to contact if there are critical issues, including security events, unplanned downtime, patient safety issues, or other critical issues as defined in the Participant Agreement	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
HIE System Upgrades	Procedure and Participant contact for CORHIO Service Desk to work with when the HIE is upgraded. HIE upgrades, including any planned downtime, are planned and communicated in advance	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
Policy and Procedure Updates	Procedure and Participant contact for CORHIO Service Desk to contact with CORHIO Policy and Procedure updates	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
Opt In/Opt Out	Participant contact to confirm receipt of opt out/opt in requests and completion of opt out/opt in	Name: Phone: Email Address:	Name: Phone: Cell/Pager: Email Address:
EHR Integration (if applicable)	Procedure and Participant contact for CORHIO Service Desk to contact with issues or communication points related to the Participant's EHR vendor or interfaces	Name: Phone: Email Address:	N/A
Participant System Upgrades	Procedure and Participant contact for CORHIO Service Desk to work with when Participant communicates an internal system upgrade or change that may impact HIE exchange	Name: Phone: Email Address:	N/A

REVISION HISTORY

Version	Date Issued	Updates Included
V1.0	Jan-11	Initial publication
V1.1	Jun-11	Updated contact sheet
V1.2	Oct-12	Updated contact sheet and procedure for participants to communicate changes to their system

Procedure: PatientCare 360 Minimum System Requirements

PURPOSE

This information outlines the minimum system requirements needed for users to operate and navigate within PatientCare 360 Community Health Record and Referral Applications.

SCOPE

This applies to all users of PatientCare 360 Community Health Record and Referral Applications.

PROCEDURE

PatientCare 360 Community Health Record Minimum System Requirements

Operating System

- Microsoft® Windows® 2000 or later

Printer Identification

- A local or network printer with factory printer drivers.

Internet Connection

- Minimum connection requirement is a 56K modem
- A broadband or high-speed connection is recommended

Web Browser

- Internet Explorer 7
- Internet Explorer 8 and 9 (in compatibility mode)
- Safari on MAC**
- Chrome, Firefox, and Mozilla *may* work, but are not explicitly supported

***Safari on a PC is NOT supported

Other Software

- Adobe Reader 9.2 or later; to view reports go to: http://get.adobe.com/reader/ for updates
- Adobe Flash Player version 10 or later; to view trended results go to: http://www.adobe.com/products/flashplayer/

Monitor Resolution

- Computer monitor should be set at a desktop resolution of 1280 x 1024 or higher

PatientCare 360 Referrals Minimum System Requirements

If the practice network is configured for proxy use, the proxy settings must be available. An existing PC or server must host the iNexx software and this machine should be an "always on" system comprised of at least:

Hardware Requirements for Windows

- Windows XP SP3, Windows 7, Windows Server 2003/2008
- Machine name must not contain special characters such as _ or and
- Pentium 4 Processor
- 1 GB RAM for Windows XP
- 2 BG RAM for Windows 7 and Windows Server 2003/2008
- Access to specific targets on the Internet over ports identified
    - https://*.novoinnovations.com (443)
    - https://healthcaredatagrid.net (443)
    - https://*.medicity.com (443)
- 10GB disk space (does not include OS, this is data storage only)

Other Software Requirements:

- Internet Explorer 7.0 or later
- Mozilla Firefox 4.0 or later
- Google Chrome 10 or later
- PDF Reader (Adobe Acrobat recommended)
- Local e-mail client

*****At this time the iNexx software is not supported by MAC systems*****

HIE PRIVACY AND SECURITY CONTROLS

CORHIO collaborates with communities and stakeholders to implement secure systems and processes for sharing clinical information. Our policies to protect the privacy and security of personal health information are developed and maintained by a statewide policy committee consisting of diverse representatives from across the Colorado healthcare community. A cornerstone of this committee is our shared commitment to privacy and security for all participants and patients in the CORHIO HIE.

Our statewide, hosted HIE infrastructure, platform, and services are provided by the joint partnership between CORHIO and Medicity.

Data Center	- HIPAA and HITECH compliant data centers (primary and backup) - SAS 70 Type II audited facility - CORHIO-specific cages - 24/7/385 hosted system monitoring and full failover capabilities - Offsite backup storage
Software and Services	- Comply with HIPAA and HITECH requirements for all services and deliverables - Annual Disaster Recovery/Business Continuity testing - Third party independent penetration testing - Up time, response time, RPE/RTO SLAs to support 24/7 operations - Intrusion detection - Anti-virus and risk assessment - Scheduled security updates
Data	- Adhere to NIST guidelines for data encryption and backup media encryption - Confederated data model – all participant data separated on edge servers maintained inside the CORHIO data center
User Access	- Role-based authorized users - Industry standards password strength and timeout requirements - User activities fully audited
Trained Workforce	- CORHIO and Medicity workforces trained and accountable for upholding laws and acts, HIPAA and HITECH compliance and any additional CORHIO HIE-specific policies. - CORHIO Security Response Team consist of a Compliance Officer, a Privacy Officer and a Security Officer.
Supporting Procedures	Internal and external policies and procedures such as: Appropriate Use of Services, Maintaining Authorized Users, Access Auditing, Inappropriate Use and Non-Compliance Reporting, System Security Safeguards, Filtering Sensitive Data, Breach Investigation and Notification
Patient Choice (Opt-Out)	Patients have the right to opt-out of participating in the HIE. Although clinical data will still flow among providers as it does today (e.g., lab results delivered to a provider from an independent lab), patients who do not wish to participate in the HIE will not have their data accessible in the community health record for query.