Title: Privacy and Security Policies

Introduction

The Coastal Connect Health Information Exchange ("CCHIE") is a not-for-profit organization that has established a voluntary electronic network (the "HIE Network") to facilitate the exchange of health information among health care providers, health plans and other health industry stakeholders. The goal of CCHIE is to assist health care organizations in improving the quality and controlling the cost of health care services through enhanced access to medical information and other clinical support.

CCHIE is committed to health information exchange that is secure and private. Accordingly, CCHIE has adopted these Privacy and Security Policies ("Policies"), which govern the use, disclosure and maintenance of health information available through the HIE Network. All individuals and entities that have access to health information through, or otherwise utilize, the HIE Network must agree to abide by these Policies.

These Policies are not designed to supersede any applicable state or federal laws or regulations, all of which continue to apply to any activities subject to these Policies. These Policies may be amended from time to time by the CCHIE Board of Directors.

These Policies are effective as of June 1, 2011.

SECTION 1: DEFINITIONS

1.1 **Authorized User** means an employee or independent contractor of a Participant, or a credentialed member of a Participant's medical or other professional staff, who has been authorized by the Participant to be a user of the HIE Network.

1.2 **Business Associate** has the meaning ascribed to this term in 45 C.F.R. § 160.103.

1.3 **Business Associate Contract** means the written agreement required by 45 C.F.R. §§ 164.502(e) containing the terms set forth in 45 C.F.R. § 164.504(e).

1.4 **Covered Entity** has the meaning ascribed to this term in 45 C.F.R. § 160.103.

1.5 **De-identified Data** means information that does not identify an Individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an Individual.

1.6 **Disclose, Disclosed, and the noun form, Disclosure** means the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information.

1.7 **Emergency Medical Condition** means a medical condition manifesting itself by acute symptoms of sufficient severity, including severe pain, such that the absence of immediate medical attention could reasonably be expected to result in (i) placing an Individual's health in serious jeopardy (ii) serious impairment to an Individual's bodily functions or (iii) serious dysfunction of any bodily organ or part of an Individual.

1.8 **Health Care Operations** means any of the following:

1.8.1 Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about Treatment alternatives; and related functions that do not include Treatment.

1.8.2 Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, Health Plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

1.8.3 Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 C.F.R. § 164.514(g) are met, if applicable.

1.8.4 Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

1.8.5 Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.

1.8.6 Business management and general administrative activities of the entity, including, but not limited to (i) management activities relating to implementation of and compliance with the requirements of HIPAA, (ii) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that Protected Health Information is not disclosed to such policy holder, plan sponsor, or customer, (iii) resolution of internal grievances, (iv) the sale, transfer, merger, or consolidation of all or part of a Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity, and (v) consistent with the applicable requirements of 45 C.F.R. § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity.

1.9 **Health Plan** has the meaning ascribed to this term in 45 C.F.R. § 160.103.

1.10 **HIE Network** means the voluntary electronic health information exchange network overseen and administered by CCHIE.

1.11 **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, as amended, and the implementing regulations at 45 C.F.R. Parts 160-164.

1.12 **Individual** means the person who is the subject of Protected Health Information.

1.13 **Joinder Agreement** means the agreement that each Participant who is not an original signatory to the Participation Agreement signs pursuant to which such Participant agrees to become a party to, and be bound by, the Participation Agreement.

1.14 **Opt Out** means the affirmative decision of an Individual or his or her Personal Representative to disallow the Individual's Protected Health Information maintained by or on behalf of one or more specific Participants from being disclosed to other Participants through the HIE Network.

1.15 **Opt Out Form** means the written or electronic document that records the decision by an Individual or his or her Personal Representative to Opt Out. Form can be accessed at www.coastalconnect.org.

1.16 **Opt Out Revocation Form** means the written or electronic document that records the decision by an Individual or his or her Personal Representative to revoke his or her decision to Opt Out. Form can be accessed at www.coastalconnect.org .

1.17 **Participant** means a Covered Entity, a Provider that is not a Covered Entity, a Business Associate of a Covered Entity or the North Carolina Division of Public Health that has executed either the Participation Agreement or a Joinder Agreement with CCHIE.

1.18 **Participation Agreement** means the written agreement entered into by at least one Participant and CCHIE governing Participants' use of the HIE Network.

1.19 **Payment means**:

1.19.1 Subject to Section 1.20.2, the activities undertaken by: (i) a Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) a health care provider or Health Plan to obtain or provide reimbursement for the provision of health care.

1.19.2 The activities in Section 1.20.1 must relate to the Individual to whom health care is provided and include, but are not limited to: (i) determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (iv) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement: (A) name and address; (B) date of birth; (C) social security number; (D) payment history; (E) account number; and (F) name and address of the health care provider and/or Health Plan.

1.20 **Personal Representative** is a person who is permitted to act on behalf of an Individual with respect to the Individual's Protected Health Information pursuant to 45 C.F.R. § 164.502(g).

1.21 **Policies** means these Coastal Connect Health Information Exchange Privacy and Security Policies.

1.22 **Protected Health Information** means information, including demographic information, collected from an Individual that: (1) is created or received by a health care provider, Health Plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and (i) that identifies the Individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. Notwithstanding the foregoing, Protected Health Information excludes (A) education records covered by the Family Educational Rights and Privacy Act, as

amended, 20 U.S.C. § 1232g; (B) records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and (C) employment records held by a Covered Entity in its role as employer.

1.23 **Provider** means (i) an entity such as a hospital, nursing home, home health agency, adult care home, mental health facility or professional corporation legally authorized to provide health care services in North Carolina, (ii) a health care professional referenced in N.C. General Statutes § 90-21.11 or a resident or student acting under the supervision of such a professional, (iii) a local health department as defined in N.C. General Statutes § 130A.-2 or (iv) mental health, developmental disabilities, and substance abuse facilities as referenced in N.C. General Statutes § 122C-3.

1.24 **Psychotherapy Notes** means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the Treatment plan, symptoms, prognosis, and progress to date.

1.25 **Public Health** means the activities described in 45 C.F.R. § 164.512(b).

1.26 **Public Health Authority** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

1.27 **Required by Law** means a mandate contained in law that compels an entity to make a use or Disclosure of Protected Health Information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

1.28 **Substance Abuse Treatment Records** means the records of federally assisted drug or alcohol abuse treatment facilities and programs that are subject to protection under 42 C.F.R. Part 2.

1.29 **Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health

care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

1.30 **Workforce** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by such entity.

SECTION 2: ELIGIBLE PARTICIPANTS

2.1 Restrictions on Use of HIE Network. Except as specified in Sections 6 and 11, CCHIE may permit only Participants and their Authorized Users to access or Disclose Protected Health Information through the HIE Network.

2.2 Covered Entities and Other Providers. The following persons or entities are eligible to be Participants:

2.2.1 Any Covered Entity.

2.2.2 Any Provider that is not a Covered Entity.

2.2.3 Business Associates that are approved by the CCHIE Board of Directors under Section 2.3.

2.3 Business Associates. A Business Associate of a Covered Entity is not eligible to be a Participant unless each of the following requirements is satisfied:

2.3.1 One or more Covered Entities that are Participants must notify CCHIE in writing that the Business Associate has a compelling need to access or Disclose Protected Health Information through the HIE Network in order to effectively perform functions for the Covered Entity that fall within the scope of a Business Associate Contract between the Covered Entity and the Business Associate.

2.3.2 CCHIE determines, in its sole discretion, that the Business Associate has a compelling need to access or Disclose Protected Health Information through the HIE Network. A compelling need shall exist only if (i) the Business Associate is performing care coordination, care management, utilization review, quality improvement or other similar services designed to improve the quality or control the cost of health care services and (ii) the inability to use CCHIE would serve as a substantial impediment to the effective performance of such services.

2.3.3 The Business Associate provides evidence to CCHIE that it maintains an office or facility in the United States and is authorized to do business in the State of North Carolina.

2.3.4 CCHIE determines, in its sole discretion, that the Business Associate has the capacity and commitment to maintain the privacy and security of Protected Health Information.

2.3.5 The Business Associate satisfies any other eligibility criteria adopted by CCHIE in its sole discretion.

2.4 Contractual Obligations. Each Participant must enter into the Participation Agreement or a Joinder Agreement and a Business Associate Contract with CCHIE to obtain authorization to access or Disclose Protected Health Information through the HIE Network.

2.5 Affiliates. Entities that control one another or are under common control may elect to participate in the HIE Network as a single Participant or multiple Participants. One entity controls another entity if the first entity has the power to appoint a majority of the members of the second entity's governing body.

2.6 Arrangements With In- and Out-of-State Exchanges and Participants.

2.6.1 CCHIE may enter into agreements with statewide, regional or local electronic health information exchanges operating in or outside the State of North Carolina under which Covered Entities or other health care providers participating in the exchange are granted the right to use the HIE Network.

2.6.2 CCHIE may enter into such agreements with only those out-of-state exchanges that are deemed by CCHIE to maintain and enforce adequate privacy and security safeguards and policies. CCHIE and the entity operating the out-of-state exchange also must enter into a Business Associate Contract.

2.6.3 Entities operating out-of-state exchanges must agree to (i) abide by the Policies and (ii) require any Covered Entities or other health care providers that gain access to the HIE Network through the exchange to abide by the Policies, except as expressly set forth otherwise in the agreement between the exchange and CCHIE. For example, application of the Policies may be waived by CCHIE if the out-of-state exchange imposes more stringent requirements on its participants or a provision of the Policies is designed to comply with a North Carolina law to which an out-of-state entity is not subject.

2.6.4 Out-of-state exchanges must authorize CCHIE or its designees to conduct off-site and on-site audits of the exchange and its participants designed to evaluate compliance with the Policies and any contractual obligations imposed by CCHIE on the exchange.

2.6.5 CCHIE is not required to directly enter into a Participation Agreement or Business Associate Contract with any Covered Entity or other health care provider that gains access to the HIE Network through an out-of-state exchange under this Section 2.6.

SECTION 3: ACCESS TO PROTECTED HEALTH INFORMATION FOR TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

3.1 Purposes for Access. Except as specified in Sections 11, Authorized Users may access Protected Health Information through the HIE Network only to carry out Treatment, Payment or Health Care Operations. Each user accessing CCHIE will have a defined role. The access policy ensures each user will only have access to information necessary to conduct activities associated with that role.

3.2 Need for Relationship With Individual. An Authorized User may access an Individual's Protected Health Information through the HIE Network to carry out Treatment, Payment or Health Care Operations only in the following circumstances:

3.2.1 CCHIE and its participating providers will have responsibilities related to access. CCHIE will make this policy known through participant outreach and education and enforce through the Participation Agreement, Joinder Agreement and/or Business Associate Agreement.

3.3 Procedure. CCHIE will use role-based access to control access levels for each user in the HIE. CCHIE will create a list of universal access roles based on the level of information necessary for care. Each participating provider organization will be responsible for assigning roles to users, as these organizations will be most familiar with the level of access needed to carry out job function. Additionally, access to patient's information will only be granted if the participant provider has an established treatment relationship with the patient (as determined by the registration process, consultation services, etc.). The only exception to this is the break glass function through which emergency users can access information in the event of an emergency or to establish a relationship with the patient for treatment purposes, if the patient has not opted-out of the HIE.

3.4 Access Model. The Patient Summary Inquiry access roles below are managed through CCHIE and Medicity; whereas, iNexx roles are managed at the provider practice level. Patient Summary Inquiry Access Roles:

COMMUNITY PROVIDER: Access to view all tabs (patient info/demographics, face sheet and documents) on Patient Summary Inquiry for patients they have an established relationship with; ability to break glass and establish a relationship with a patient therefore removing the break glass requirement during the established relationship time; ability to create a Continuity of Care document.

ED PROVIDER: Access to all tabs/information without having to break glass; ability to create a Continuity of Care document.

COMMUNITY STAFF W/ QUERY: Access to view all tabs of patients their provider(s) have a relationship with; ability to break glass; cannot establish a relationship with the patient therefore must break glass with each access; ability to create a Continuity of Care document.

SECTION 4: MINIMUM NECESSARY REQUIREMENT

4.1 Obligations of Authorized Users. Subject to Section 4.2, Authorized Users must make reasonable efforts to access and use only the minimum amount of Protected Health Information available through the HIE Network that is necessary to carry out the authorized purpose for which such Protected Health Information is accessed or used.

User Authorization. Authorization assures the confidentiality of health information by requiring CCHIE to verify the access role a user is assigned. This policy sets forth the minimum requirements for authorized users of the HIE. Upon individual participant authentication and access to CCHIE, CCHIE must verify which functions that a user is authorized to perform. CCHIE shall assign participants access roles. Participants shall be authorized to access health information consistent only with the functions defined by the access roles. CCHIE and its participating providers will have responsibilities related to authorization. CCHIE will make this policy known through participant outreach and education, and enforced through the participation agreement, joinder agreement and business associate agreement.

CCHIE shall allow individual participants to access health information based upon the access role assigned to them by CCHIE. At present, authorization of access to health information is limited to treatment, payment for treatment and health care operations.

1. *Role-based Access:* CCHIE will assign participants user access roles. Participants shall only be authorized to access the HIE in compliance with the assigned role definition.
2. *Creation and Management of Users:* CCHIE will be responsible for the creation and management of users who access the HIE. User Authorization will be managed by ensuring that requests for new users come from participant verified "super-users" with the ability to submit new user requests. No user will be authorized to access the exchange unless the request to create that user originates from the participant's "super-user" and/or authorized designee.
3. *Physician Address Book:* CCHIE will be responsible for ensuring that all of the necessary user information is present for a complete entry into the physician address book or other user database.
4. *Unauthorized Access:* All access not consistent with CCHIE policies shall be deemed unauthorized. Unauthorized access shall set forth immediate termination of access privileges and may be subject to other penalties by CCHIE.

New user accounts are created with the approval of the practice lead and with new user's execution of a Confidentiality and Password Agreement.

4.2 Treatment Exception. The obligations set forth in this Section 4 do not apply to the access to or use of Protected Health Information by a Provider for Treatment.

4.3 Reliance on Access Requests. A Participant making a Disclosure of Protected Health Information through the HIE Network may rely on compliance with this Section 4 by

Participants accessing Protected Health Information through the HIE Network. A Participant making such a Disclosure is not required to take any additional steps to restrict the availability of its own Protected Health Information through the HIE Network, except as expressly required by other provisions of the Policies or applicable law.

4.4 Minimum Necessary Policies and Criteria. Each Participant must establish protocols designed to limit the amount of Protected Health Information accessed by its Authorized Users for recurring and routine purposes to the amount necessary to carry out the authorized purpose. Each Participant must establish criteria governing the amount of Protected Health Information accessed by its Authorized Users for other purposes that are designed to limit such access to the amount of Protected Health Information necessary to carry out the authorized purpose.

4.5 Record Searches. When searching any master patient index, record locator service or other similar system made available by CCHIE to locate records about an Individual through the HIE Network, an Authorized User must follow any search guidelines established by CCHIE and make reasonable efforts to minimize instances in which the Protected Health Information of the wrong Individual is inadvertently accessed by the Authorized User.

4.6 Help Desk. CCHIE may provide technical support to participants using a variety of resources, including telephone, email, or web-based chat tools and remote assistance technology. Technical support is available Monday through Friday, from 8:00am until 5:00pm EST. Users may request technical support by calling our toll free support line at 888-213-2147, sending an email to support@coastalconnect.org, or visiting our Help Desk on the web at http://support.coastalconnect.org.

SECTION 5: EMERGENCY ACCESS, AUTHENTICATION AND AUDITING

5.1 Standards for Emergency Access. Authorized Users may access Protected Health Information maintained by Participants about an Individual who has exercised his or her right to Opt Out of Disclosures by such Participants if all of the following requirements are satisfied:

5.1.1 The reasonably apparent circumstances indicate to the Authorized User that (i) the Individual has an Emergency Medical Condition; (ii) a meaningful discussion with the Individual or his or her Personal Representative about whether to rescind a previous decision to Opt Out is impractical due to the nature of the Individual's Emergency Medical Condition; and (iii) information available through the HIE Network could assist in the diagnosis or Treatment of the Individual's Emergency Medical Condition.

5.1.2 The Authorized User obtains access to the HIE Network through a Provider that is treating or diagnosing the Individual's Emergency Medical Condition.

5.1.3 The Authorized User is involved in providing or arranging for the diagnosis or Treatment of the Individual's Emergency Medical Condition.

5.1.4 Attestation. CCHIE shall ensure that the Protected Health Information of Individuals who have exercised their right to Opt Out is not accessible to Authorized Users under this Section 5 unless the Authorized User seeking such access provides an attestation electronically through the HIE Network at the time he or she requests access stating that all of the conditions specified in Section 5.1 are satisfied. All such attestations shall be stored electronically by CCHIE for a period of at least six years.

5.1.5 Termination of Emergency Access. Authorized Users shall cease emergency access of an Individual's Protected Health Information under this Section 5 promptly upon (i) stabilization of the Individual's Emergency Medical Condition or (ii) a request by the Individual or his or her Personal Representative to cease such access.

5.2 User Authentication. Authentication assures the confidentiality of health information by requiring that the identities of all individual participants of CCHIE are verified when accessing the HIE. This policy sets forth the actions required for participant authentication when attempting to access the statewide HIE and to establish standards for authentication. CCHIE and its participating providers will have responsibilities related to authentication. CCHIE will make this policy known through participant outreach and education, and enforce through the participation agreement, joinder agreement and business associate agreement. CCHIE will utilize single-factor authentication (user name and strong password) for access to the HIE.

5.2.1 User Name Convention

User Names will consist of the first letter of the user's first name, and the user's full last name (or truncated version of the last name if it is longer than 12 characters). Example John Doe = "JDoe"

If the user name of a new user is identical to that of an existing user, the second letter of the new user's first name will be inserted after the first letter. If after all the letters in a user's first name are utilized an identical user name still exists, than a number will be appended after the last name, starting with the number 1. Example Jane Doe = "JaDoe", Johnny Doe = "JoDoe" and Jo Doe = "JoDoe1"

5.2.2 Password Convention

For Patient Summary Inquiry Users, passwords must be at least six (6) characters, contain a minimum of one (1) UPPER case letter and one (1) number; must not contain four (4) consecutive characters that are consecutive in the user's username (user name: JDoe, password JDoe1 not allowed); must not contain the name of the user's organization; must not contain the following words/phrases "CCHIE", "HIE", "password"); and must not be identical to any of the user's previous passwords. An encrypted record of all users' previous passwords will be kept in order to ensure a user does not duplicate their previous passwords.

For iNexx users, the password must be at least 5 characters. There can be upper, lower case, numbers and symbols. There is no default configuration.

5.2.3 Authentication Attempts

Authentication must be provided at every access attempt. CCHIE shall record all authentication access attempts. After five (5) consecutive failed log-in attempts a user will be locked out. The lock-out will be terminated only after the user's identity is verified and their password is reset. The user must submit a support ticket to CCHIE helpdesk. This can be can be done by either emailing the unlock request to support@coastalconnect.org or go to www.coastalconnect.org and click on the live help link.

5.2.4 Password Changes

A user will be able to reset their password (via the CCHIE portal) according to the preset criteria of each application. A user will have to change their password every six (6) months when prompted by the program. Users will be reminded to change their password upon logging into the application, but not via third party EMR. Access to the exchange via third-party EMR will not be affected by a user's password status.

5.2.5 Authentication Data

CCHIE shall ensure authentication data is secure at the time it is entered and is administered safely. CCHIE shall ensure the safety and identity of active and non-active participant user names and passwords. The practice should inform CCHIE of personnel changes (additions and deletions).

5.2.6 Authentication Violation

CCHIE Participants are responsible for reporting to CCHIE participant individual suspected activity in violation of CCHIE authentication policies or any participant individual activity that may cause harm to the HIE or its participants. Reporting can be done by emailing support@coastalconnect.org.

5.3 Auditing. The purpose of the audit policy is to provide ongoing monitoring of compliance with all applicable laws, regulations, and CCHIE policies. The ability to execute periodic and ad hoc audits gives CCHIE the ability to monitor participating providers' compliance with CCHIE contractual requirements and, if detected in the course of such monitoring, violation of legal regulatory requirements. If CCHIE does find that a participating provider is in violation of its contract, CCHIE will take prompt action to enforce the contract with the participating provider. CHIE is not responsible for nor obligated to monitor general legal or regulatory compliance by its participating providers. However, CCHIE will take what it deems to be reasonable steps, typically notification of the participating provider, if such violations are detected during the course of an audit. CCHIE and its participating providers will have responsibilities related to audit. CCHIE will make this policy know through participation outreach and education and enforce through the participation agreement, joinder agreement and business associate agreement. CCHIE will maintain an audit trail as a mechanism to demonstrate compliance with participant use and disclosure authorizations(s). The audit trail will contain date-, time-, and source-stamped historical records of activities and transactions that pertain to CCHIE access and the use and disclosure of personal health information available through the HIE. Entry will be immutable (unchanging and unchangeable) in content. CCHIE will maintain an active audit trail for the previous six months, with an archive of three years of audit information. Provider audits should be ongoing in order to ensure patient information is kept secure.

5.3.1 Break glass. A separate audit log will be stored for "Break Glass" instances where a user is required to gain further information on a patient that does not yet have a clinical relationship established to a participating provider within CCHIE. In addition, certain case management entities will be subject to a user-by-user audit to determine proper usage of the system.

5.3.2 **ProAccess (Patient Summary Inquiry - PSI)**. A separate audit log is stored for ProAccess use. An audit is run to determine user logins for the previous month. From that report a sample size of no less than 5% of users is randomly selected. A report is then run on unique patients accessed by each user. The criteria reviewed include matching last names of patients searched and user searching, pediatricians searching patients other than children, and geriatric practices searching younger patients. Any suspicious activity will be reported to individual practices.

5.3.3 **Quarterly Physician Practice Audit.** A quarterly audit will be performed to maintain updated user lists for each practice. A report of active users is run for each practice and sent to practice lead for confirmation. Practice lead provides

updates, ie. a staff member no longer working at a practice, or signs the report confirming an accurate record of their users and returns to CCHIE. Any changes noted are made by CCHIE.

SECTION 6: ACCESS RIGHTS OF CCHIE WORKFORCE

6.1 Authorized Purposes. CCHIE may authorize its own Workforce to access Protected Health Information through the HIE Network only to the extent consistent with the terms of CCHIE's Business Associate Contracts with Participants and only for one or more of the following purposes:

6.1.1 To facilitate the Disclosure of Protected Health Information to Participants or for Public Health purposes as permitted by the Policies.

6.1.2 To process or otherwise implement Opt Out requests.

6.1.3 To perform patient identity or patient records maintenance.

6.1.4 To conduct or assist in the performance of audits permitted or required by the Policies, including audits of Emergency Access required by Section 5.

6.1.5 To perform data analysis on behalf of and at the request of one or more Participants, to the extent consistent with HIPAA and the Policies.

6.1.6 To evaluate the performance of or develop recommendations for improving the operation of the HIE Network.

6.1.7 To conduct technical system support and maintenance on the HIE Network.

6.1.8 To engage in any other activities reasonably related to the operation of the HIE Network that are authorized by CCHIE Board of Directors and are consistent with applicable law.

6.2 Role-Based Access. CCHIE shall establish role-based access standards reasonably designed to enable each Workforce member to access only such Protected Health Information that is necessary for the performance of his or her authorized activities. These standards shall ensure that CCHIE Workforce members access and use only the minimum necessary amount of Protected Health Information reasonably required to carry out the authorized purpose.

6.3 Training. No CCHIE Workforce member may access Protected Health Information through the HIE Network unless the Workforce member has received training regarding the policies.

6.4 Discipline for Non-Compliance. CCHIE shall discipline Workforce members who violate the Policies or engage in any other unauthorized or inappropriate behavior that undermines the privacy or security of Protected Health Information available through the HIE Network. Depending on the circumstances, disciplinary measures may include verbal and written warnings, retraining, demotion, suspension or termination of employment.

6.5 Reporting and Non-Retaliation. CCHIE shall require all Workforce members to report any actual or suspected violation of the Policies of which they become aware. No Workforce member may be subject to retaliation of any kind for reporting a violation in good faith.

6.6 Business Associates. CCHIE may authorize its own Business Associates to access Protected Health Information for a purpose that is consistent with Section 6.1, provided CCHIE has entered into a Business Associate Contract with the Business Associate.

SECTION 7: OPT OUT RIGHTS

7.1 Right of Individuals to Opt Out. An Individual may elect to Opt Out at any time. An Individual may Opt Out of having CCHIE Disclose (i) the Individual's Protected Health Information obtained through the HIE Network from all Participants or (ii) the Individual's Protected Health Information obtained through the HIE Network from those Participants the Individual lists on the Opt Out Form. A Personal Representative may Opt Out on behalf of an Individual.

7.2 Use of Opt Out Form. CCHIE shall develop an Opt Out Form to facilitate an individual's decision to Opt Out. CCHIE's Opt Out form is available at www.coastalconnect.org. The Opt Out Form may be amended by CCHIE from time to time with the approval of CCHIE Board of Directors.

7.3 Contents of Opt Out Form.

7.3.1 The Opt Out Form shall include the following information:

a. A notice that Participants are authorized to Disclose an Individual's Protected Health Information through the HIE Network unless and until the Individual elects to Opt Out by completing and submitting the Opt Out Form.

b. A notice that an Individual's decision to Opt Out will not prevent Participants from Disclosing an Individual's Protected Health Information through the HIE Network for Public Health or Research purposes.

c. A notice that an Individual's decision to Opt Out will not affect the Individual's right to receive health care services or benefits from Participants.

d. An explanation of:

i. The purpose and basic functions of the HIE Network.

ii. The types of Protected Health Information that are exchanged through the HIE Network.

iii. The types of Participants that may Disclose and access Protected Health Information through the HIE Network.

iv. The purposes for which Protected Health Information is exchanged through the HIE Network.

v. The effect of a decision to Opt Out on Providers' access to Protected Health Information to treat an Emergency Medical Condition.

vi. How to submit an Opt Out Form.

vii. Where to obtain additional information about the HIE Network.

7.3.2 The Opt Out Form shall contain the following elements:

a. A field in which the Individual may indicate that he or she is electing to prohibit all Participants from accessing his or her Protected Health Information through the HIE Network.

7.3.3 The Opt Out Form shall include the demographic information determined by CCHIE Board to be necessary for accurate matching of Individuals in the HIE Network.

7.4 Processing of Opt Out Requests by CCHIE.

7.4.1 CCHIE shall post the Opt Out Form prominently on its website. CCHIE shall permit Individuals or their Personal Representatives to complete and submit the Opt Out Form by mail or fax.

7.4.2 Upon receipt of an Opt Out Form by mail or fax, CCHIE will contact the patient to confirm request. CCHIE shall maintain records of all Opt Outs for six years.

7.4.3 CCHIE shall prepare patient talking points to distribute to connected providers to support patient education around the HIE.

7.5 Opt Out Notification by Participants.

7.5.1 Provider Participants that provide face-to-face Treatment to Individuals shall update their practice privacy statements to include language around the electronic exchange of clinical information through the HIE.

7.6 Implementation of Opt Outs. CCHIE shall employ technical measures to prevent the Disclosure of any Protected Health Information through the HIE Network that is subject to an Opt Out. Such measures shall be implemented within two business days of the completion of the Opt Out verification process described in this Section 7. Notwithstanding the foregoing, CCHIE may permit Protected Health Information subject to an Opt Out to be Disclosed through the HIE Network to provide Treatment for a Medical Emergency Condition in accordance with Section 5, for Research in accordance with Section 11 or for Public Health in accordance with Section 13.

7.7 Opt Out Revocation Process.

7.7.1 An Individual or his or her Personal Representative may revoke his or her decision to Opt Out at any time.

7.7.2 CCHIE shall develop an Opt Out Revocation Form. CCHIEs Revoke Opt Out form is available at www.coastalconnect.org. The submission of an Opt Out

Revocation Form in accordance with this Section 7 shall be the sole means by which an Individual may revoke his or her decision to Opt Out. No Participant shall use any other mechanism to revoke an Individual's decision to Opt Out. The Opt Out Revocation Form may be amended by CCHIE from time to time with the approval of CCHIE Board of Directors.

7.7.3 The Opt Out Revocation Form shall include the elements relating to the Individual included in Section 7.3.3 and shall be distributed and collected according to the methods set forth in Section 7.4.

7.8 Maintenance of Protected Health Information in HIE Network. A Participant may maintain a copy of its Protected Health Information in a computer system operated by CCHIE without regard to whether an Individual has elected to Opt Out.

7.9 Restrictions on the Disclosure of Certain Information. If Protected Health Information is not subject to an Opt Out, such information may be Disclosed through CCHIE for any purpose permitted by the Policies, except that Participants shall not include Psychotherapy Notes, Substance Abuse Treatment Records, or other information that may not be Disclosed without a patient's authorization under federal law in the Protected Health Information made available through the HIE Network unless (i) the Individual or his or her Personal Representative has signed an authorization form that complies with applicable law permitting the Disclosure of such information and (ii) the information is identified in the HIE System as subject to restrictions on re-disclosure absent additional authorization.

SECTION 8: DATA USE AND DATA RENTION

8.1 Data Use. It is the policy of CCHIE that data contained and transported through the exchange belongs to its subscribing organizations. CCHIE exists to serve the health information exchange and transport needs of its subscriber members and as such will never sell, provide access to, or utilize that data to benefit itself or any third party entities, without the express written permission of the affected subscriber organizations.

8.1.1 Responsibilities of CCHIE. CCHIE exists for the open and free exchange of health information for the purposes of treatment, payment, or healthcare operations. All subscribers to CCHIE are required to fully comply with all provisions described in the CCHIE Participation Agreement, Joinder Agreement and/or Business Associate Agreement.

8.1.2 All Participating Organizations must comply with all CCHIE Policies and Procedures.

8.1.3 All Participating Organizations must comply with the all laws for privacy, security and use of Patient Data imposed under the laws of the United States, the State of North Carolina, and any other states with jurisdiction over the issue.

8.2 Data Retention. It is the policy of CCHIE to govern the historical time period that electronic clinical/medical records will be retained within the CCHIE infrastructure, as well as data source databases. The policy establishes controls to ensure the proper management of electronic medical records, which are the property of the subscribing organizations, and are required to satisfy both federal and North Carolina regulatory requirements. This policy applies to all participants of CCHIE that have registered with and are participating in CCHE and its workforce members including employees, medical staff, contractors and volunteers. Medical records shall be retained or archived to support the policies and procedures of the subscribing organizations.

8.2.1 Connected Practices. It is the sole responsibility of the practice or provider receiving clinical data to maintain backup copies of any relevant or necessary data to the extent required by the authorized user, authorized user's organization, or governmental regulation.

SECTION 9: BREACH

9.1 **Breach** shall mean the acquisition, access, Disclosure, or use of Patient Information through the HIE Network in a manner not permitted by the HIPAA Regulations or this Agreement which compromises the security or privacy of such Patient Information. The term "Breach" shall not include any unintentional acquisition, access, Disclosure, or use of Patient Information by an employee or individual acting under the authority of CCHIE or a Participant or Authorized User if:

9.1.1 Such acquisition, access, Disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with CCHIE, a Participant or an Authorized User, and

9.1.2 Such Patient Information is not further acquired, accessed, used, or Disclosed by such employee or individual.

9.1.3 The term Breach also shall not include any acquisition, access, Disclosure or use of Patient Information contained in or available through the Participant's System where such acquisition, access, Disclosure or use was not directly related to Disclosure of Patient Information through the HIE Network.

9.2 Breach Notification.

9.2.1 Responsibilities of Participants. Participants must notify CCHIE if they become aware of any actual or suspected Breach through the HIE Network. Except as otherwise provided in the CCHIE Privacy and Security Policies, notification shall be made within three (3) days of a Participant's learning of the actual or suspected Breach.

9.2.2 Responsibilities of CCHIE. If CCHIE becomes aware of any actual or suspected Breach, either through notification by a Participant or otherwise, CCHIE must, at a minimum, within three (3) days of learning of the actual or suspected Breach, notify any Participants whose Patient Information is or may be affected by the Breach.

a. Contents of Notification. The notification required by this Section10 shall include sufficient information for CCHIE and notified Participants to understand the nature and extent of the Breach. For instance, such notification should include, to the extent available at the time of the notification, the following information:

b. A brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;

c. The identification of each Individual whose Patient Information has been, or is reasonably believed to have been, accessed, acquired, used, or Disclosed during the Breach;

d. Description of the roles of the people involved in the Breach (e.g., employees, Authorized Users, service providers, unauthorized persons, etc.);

e. Description of the types of Patient Information that were involved in the Breach (whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

f. Description of Participants likely impacted by the Breach;

g. Number of Individuals or records impacted/estimated to be impacted by the Breach;

h. Description of actions taken to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breach;

i. Current status of the Breach (under investigation or resolved);

j. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address; and

k. Corrective action taken and steps planned to be taken to prevent a similar Breach.

9.1.3 The notifying party shall have a duty to supplement the information contained in the notification as it becomes available and to cooperate with other Participants and CCHIE in mitigating the effects of the Breach. Except as provided for in Section 10(c)(ii), the notification required by this Section 10 shall not include any Patient Information.

9.1.4 CCHIE will provide, in a timely manner, a summary of the Breach to such Participants that does not identify any of the Participants or Individuals involved in the Breach.

9.1.5 This Section 10 shall not be deemed to supersede or relieve a party's reporting obligations (if any) under relevant security incident, breach notification or confidentiality provisions of Applicable Law, including, but not limited to, those related to Individuals.

9.1.6 The parties shall work together to coordinate any notification to Individuals, any applicable regulatory agencies, and any public announcement regarding the Breach that may be required by Applicable Law or the policies of a party. Notwithstanding the foregoing, the party that is legally required to make the notification and/or public announcement shall have final approval of the contents of any such notification or announcement.

10 ACCOUNTINGS OF DISCLOSURES

10.1 Tracking of Disclosures by CCHIE. CCHIE shall ensure that the HIE Network has the capacity to track all Disclosures of each Participant's Protected Health Information made through the HIE Network. Disclosures shall be tracked in accordance with the following standards:

10.1.3 If the Disclosure is from one Participant to another Participant for Treatment, Payment or Health Care Operations, a record of the Disclosure must be maintained by CCHIE for three years from the date of the Disclosure. The information tracked for each such Disclosure shall be sufficient to enable a Participant to provide an accounting to the Individual that complies with HIPAA.

10.1.4 If the Disclosure is from CCHIE to another party for Public Health, Research or any other purpose permitted by the Policies, a record of the Disclosure must be maintained by CCHIE for six years from the date of the Disclosure. The information tracked for each such Disclosure shall include:

10.1.4.1 The date of the Disclosure;

10.1.4.2 The name of the entity or person who received the Protected Health Information and, if known, the address of such entity or person;

10.1.4.3 A brief description of the Protected Health Information disclosed; and

10.1.4.4 A brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure.

10.2 Requests for Accountings by Participants.

10.2.3 A Participant may request that CCHIE provide the Participant with an accounting of Disclosures of an Individual's Protected Health Information made through the HIE Network to enable the Participant to respond to a request for an accounting by the Individual or his or her Personal Representative under HIPAA. Participants must make such requests in accordance with procedures and utilizing forms adopted by CCHIE.

10.2.4 CCHIE shall be obligated to provide an accounting of those Disclosures made through the HIE Network within the following time periods:

10.2.4.1 If the Disclosure is from one Participant to another Participant for Treatment, Payment or Health Care Operations, the accounting must include at least those Disclosures made during the three year period immediately preceding the date of the Individual's request.

10.2.4.2 If the Disclosure is from CCHIE to another party for Public Health, Research or any other purpose permitted by the Policies, the accounting must

include at least those Disclosures made during the six year period immediately preceding the date of the Individual's request.

10.2.5 CCHIE shall respond to all requests for accountings by Participants within 30 days of CCHIE's receipt of the request. CCHIE's response shall include, for each Disclosure for which an accounting must be provided, all of the information CCHIE is obligated to track under Section 9.1.

10.3 Accounting Requests by Individual. Upon the receipt of accounting requests from Individuals or their Personal Representatives, CCHIE shall forward the request to all Participants whose Protected Health Information is subject to the request and notify the Individual or Personal Representative that such Participants will be preparing a response. In those cases where Individuals or Personal Representatives prefer not to receive a response from the Participants, the CCHIE Board of Directors will establish guidelines under with Individuals or Personal Representatives can request accounting information directly from the CCHIE.

10.4 Exemption from Accounting Requirement. CCHIE shall not be responsible for tracking or providing Participants with an accounting of any Disclosures exempt from the HIPAA accounting requirement under 45 C.F.R. § 164.528 (a)(ii)-(ix).

11 RESPONDING TO SUBPOENAS AND DISCOVERY REQUESTS

11.1 Disclosures In Response to Court Orders. CCHIE may Disclose Protected Heath Information in its possession in response to a court order provided CCHIE Discloses only the Protected Heath Information expressly authorized by such order.

11.2 Disclosures in Response to Subpoenas and Discovery Requests.

11.2.3 Subject to Section 12.3, CCHIE may Disclose Protected Heath Information in its possession in response to a subpoena, discovery request or other lawful process that is not accompanied by an order of a court only if the subpoena, discovery request or other lawful process is accompanied by a written authorization from the Individual who is the subject of the requested Protected Health Information.

11.2.4 CCHIE shall respond to subpoenas, discovery requests or other lawful processes that do not satisfy the requirements of Section 12.1 or 12.2.1 by transmitting a written objection to the party requesting the Protected Health Information setting forth the need for either a court order or a written authorization from the Individual in connection with such request.

11.3 Opportunity for Participants to Resist Request. CCHIE shall notify all Participants whose Protected Health Information is subject to a potential Disclosure under Section 12.2 of CCHIE's intention to make the Disclosure no less than five days prior to the anticipated date of the Disclosure. CCHIE shall not Disclose any Participant's Protected Health Information if (i) the Participant notifies CCHIE within such five-day period of the Participant's intention to move to quash the subpoena or otherwise resist the request and (ii) the Participant takes such action within the time period necessary to prevent CCHIE from failing to comply with any legal duty to which it is subject. CCHIE shall not make any Disclosure under this Section 12 to the extent any request for Protected Health Information is withdrawn by the requesting party or rejected by a court or administrative tribunal in response to an objection by a Participant.

11.4 No Obligation to Search Participant Records. Under this Section 12, CCHIE shall Disclose only those records under its custody and control. CCHIE shall not Disclose any records CCHIE may be capable of obtaining by conducting searches through the HIE Network of the records maintained by Participants in their own record systems.

11.5 Consultation With Counsel. CCHIE shall consult with its counsel regarding its authority to Disclose Protected Health Information under this Section 12 prior to making any such Disclosure.

11.6 Minimum Necessary. CCHIE shall Disclose only the minimum necessary Protected Heath Information in response to requests covered by this Section 12.

11.7 Verification of Identity. CCHIE shall verify the identity and authority of the requesting party prior to Disclosing Protected Heath Information under this Section 12.

11.8 Accounting of Disclosures. CCHIE shall maintain a record of Disclosures made under this Section 12 in accordance with Section 9.1.2 of the Policies.

12 ACCESS TO DATA BY GOVERNMENT AGENCIES

12.1 Disclosures Required by Law. CCHIE may Disclose Protected Health Information to a government agency or its representatives or agents when the Disclosure is Required by Law. Nothing in this Section 13.1 shall be construed as obligating CCHIE to Disclose Protected Health Information to a government agency on behalf of a Participant when the Participant, rather than CCHIE, is Required by Law to make the Disclosure.

12.2 Disclosures for Public Health Purposes. CCHIE may Disclose Protected Health Information to Public Health Authorities for Public Health purposes. CCHIE's Board of Directors shall approve the general types of Public Health purposes for which Protected Health Information may be Disclosed under this Section 13.2.

12.3 Minimum Necessary. CCHIE shall Disclose only the minimum necessary Protected Health Information for the purposes specified in Section 13.1 or 13.2. CCHIE may rely on a public health official's or other government official's determination that the information requested represents the minimum necessary for the requested purpose.

12.4 Verification. CCHIE shall verify the identity and authority of the representative or agent of the government agency making the request prior to Disclosing Protected Health Information for the purposes specified in Section 13.1 or 13.2.

12.5 Accounting of Disclosures. CCHIE shall maintain a record of Disclosures made under Section 13.1 or 13.2 in accordance with Section 9.1.2 of the Policies.

12.6 Participant Notification. Except as restricted by applicable law, CCHIE shall promptly notify Participants whose Protected Heath Information has been Disclosed by CCHIE under Section 13.1.

12.7 Other Disclosures Not Permissible. CCHIE shall not Disclose Protected Health Information to government agencies or their representatives or agents for any purpose not permitted by this Section 13 or another provision of the Policies.