NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

NC HealthConnex
Powering Health Care Outcomes

North Carolina Health Information Exchange Authority

User Access Policy for NC HealthConnex

North Carolina Health Information Exchange Authority

User Access Policy for NC HealthConnex

Introduction

The North Carolina Health Information Exchange Authority ("NC HIEA") is an agency of the State of North Carolina, housed within the Department of Information Technology's Government Data Analytics Center (GDAC). The North Carolina General Assembly created the NC HIEA and directed it to establish an electronic state-wide health information exchange network, known as NC HealthConnex, to facilitate the exchange of health information among health care providers, health plans, and other health industry stakeholders. See N.C.G.S. §§ 90-414.1, et seq., and NC Session Law 2015-241 §§ 12A.4 and 12A.5. The goal of the NC HIEA is to assist health care organizations and health plans in improving the quality and controlling the cost of health care services through enhanced access to medical information and other clinical support. To support that goal, the legislation requires all providers of Medicaid and state-funded services to be connected to NC HealthConnex by specific dates based on provider and service type. Certain health plans and business associates may also be required to connect to or access NC HealthConnex.

The NC HIEA is committed to health information exchange that is secure and private. Accordingly, the NC HIEA has adopted these User Access Policies (together with the NC HIEA Privacy & Security Policies, the "Policies"), which govern Participants' access and use of health information available through NC HealthConnex. All individuals and entities that have access to health information through, or otherwise utilize, NC HealthConnex must abide by these Policies.

These Policies do not supersede any applicable state or federal laws or regulations, all of which continue to apply to any activities described in these Policies. From time to time the NC HIEA, in consultation with its Advisory Board, may amend these Policies. Definitions include references to laws or regulations as appropriate to illustrate the context and intent of this Policy.

These updated Policies are effective as of April 5, 2021 (proposed).

SECTION 1: Definitions

1.1 **Applicable Law** means all applicable statutes and regulations of the State in which the Participant operates, as well as all applicable Federal statutes, regulations, standards and policy requirements.

1.2 **Authorized User or 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 NC HealthConnex and services, such as the Clinical Portal or DSM.

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

1.4 **Business Associate Agreement** 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).

1.5 **Clinical Portal or Portal** means the web-based user interface that Authorized Users can utilize to access their patients' medical records and to use NC HealthConnex services and features.

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

1.7 **DirectTrust** means the collaborative non-profit association of health information technology and health care provider organizations to support secure, interoperable health information exchange via Direct Secure Message protocols.

1.8 **Direct Secure Messaging or DSM** means the encrypted messaging service that can be provided to Participants by the NC HIEA, a certified Health Information Service Provider, that allows Participants to communicate securely with other NC HealthConnex Participants or with other certified Direct Secure Message recipients.

1.9 **HIE Data** means the data submitted to NC HIEA as required by N.C.G.S. §90-414.4, together with such other PHI, or Message Content, as may be necessary or proper to achieve the purposes of the NC HIEA in N.C.S.L. 2015-241.

1.10 **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended, and the implementing regulations at 45 C.F.R. Parts 160 through 164.

1.11 **Message** means an electronic transmission of Message Content Transacted between Participants. Messages are intended to include all types of electronic transactions, including the data or records transmitted with those transactions.

1.12 **Message Content** means that information contained within a Message or accompanying a Message. This information includes, but is not limited to, Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonymized data, metadata, Digital Credentials, and schema.

1.13 **NC HealthConnex** means the electronic health information exchange network overseen and administered by the NC HIEA.

1.14 **NC HIEA** means the North Carolina state agency created to operate the statewide electronic health information exchange network pursuant to N.C.G.S. § 90-414.7.

1.15 **Participant** means a Covered Entity, a health care provider that is not a Covered Entity, a Business Associate of a Covered Entity, or an agency of the State of North Carolina that has executed a Participation Agreement with the NC HIEA.

1.16 **Participant Access Policies** means the policies and procedures of a Participant that govern the ability of Participant Authorized Users to transact information using NC HealthConnex.

1.17 **Participant Account Administrator or PAA** means the staff member(s) employed by Participant or Participating Entities who will be authorized to assign user credentials to Authorized Users within the Participant organization for NC HealthConnex and Direct Secure Messaging. The Participant Account Administrator will also be the main contact person who will receive communication from the NC HIEA and who will coordinate the collaboration between NC HIEA's technology vendor and the Participant's technical services contact.

1.18 **Participation Agreement** means the written agreement entered into by at least one Participant and the NC HIEA governing Participants' use of NC HealthConnex.

1.19 **Protected Health Information or PHI** has the meaning assigned to this term in 45 C.F.R. § 160.103.

1.20 **Provider Directory** means a directory of the secure email addresses of NC HealthConnex Participants and North Carolina providers participating in DirectTrust.

1.21 **Transact** means to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content through NC HealthConnex or the nationwide eHealth Exchange.

1.22 **Workforce** has the meaning assigned to this term in 45 C.F.R. 160.103.

SECTION 2: User Authorization & Access Roles

2.1 **Procedure.** The NC HIEA uses role-based access to control access levels for each Authorized User in NC HealthConnex. The NC HIEA has created a list of universal access roles based on the level of information necessary for the provision of care. From time to time, the NC HIEA may revise the access roles. Each Participant Account Administrator is responsible for assigning roles to users because organizations are most familiar with the level of access needed to carry out job function. Additionally, access to a patient's information is only granted if the Participant's Authorized User 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 the Seal" function through which participants can establish a relationship with a patient if the patient has not opted out of NC HealthConnex.

2.2 **Portal User Authorization.** This policy sets forth the minimum requirements for Authorized Users of the NC HealthConnex Clinical Portal. Authorization assures the confidentiality of health information by requiring the Participant Account Administrator to verify the access role a user is assigned. Authorized Users shall be authorized to access health information consistent only with the functions defined by the access roles. NC HIEA can enforce these obligations pursuant to the Participation Agreement and/or Business Associate Agreement.

2.2.1 NC HIEA shall allow Authorized Users to access health information based upon the access role assigned to them. Authorization of access to health information is limited to treatment, payment for treatment and health care operations as well as the Permitted Purposes provided in the NC HIEA Participation Agreement. New user accounts are created with the approval of the NC HIEA Help Desk.

a. **Role-based Access:** All Authorized Users must be assigned to a role relevant to his or her position in the Participant organization. Participants shall only be authorized to access NC HealthConnex in compliance with the assigned role definition. These roles are referenced in section 2.3 of this document.

b. **Creation and Management of Users:** The Participant Account Administrator at each Participant organization will be responsible for the management of users who access NC HealthConnex. No user will be authorized to access NC HealthConnex unless the NC HIEA Help Desk has given the user the required credentials to access NC HealthConnex.

c. **Restrictions of User Authorization:** The Participant Account Administrator must abide by the Participation Agreement when requesting access for their organization's Workforce members to NC HealthConnex and all NC HealthConnex Services, including Direct Secure Messaging and NC*Notify**. Participant Account Administrators are not authorized to give user credentials to persons not included in the Participant's Workforce or to persons or entities that are not Workforce members of the Participating Entities under control of the Participant organization.** Doing so is a breach of the Participation Agreement and may involve termination or suspension of Participant's connection and access to NC HealthConnex.

d. **Unauthorized Access:** All access not consistent with the NC HIEA Participant Agreement and Policies shall be deemed unauthorized. Unauthorized access shall set forth suspension or termination of access privileges and may be subject to other penalties by the NC HIEA. Any and all access not consistent with the NC HIEA Participant Agreement and Policies shall be deemed "unauthorized access." Such unauthorized access may result in suspension or termination of access privileges and/or other penalties assessed by the NC HIEA. Further, unauthorized access that violates applicable laws and regulations may result in other legal penalties.

2.3 **Access Model.** NC HealthConnex is configured with various clinical views that Authorized Users may access. Not all views need to be accessed by all users, and access can be based on sensitivity of information or relevance to the Authorized Users. User groups and roles are used to control this access. One Authorized User should be assigned to one level based on the individual's role within the Participant organization. See Table 1 for Clinical Portal User Levels and Roles and relevant descriptions. An Authorized User who has completed the CSRS enrollment process for integration via NC HealthConnex will also have a CSRS role assigned to them. See Table 3 for CSRS user roles and their descriptions.

2.4 **Functions Based on Authorized User Level.** The ability of Authorized Users to view certain types of clinical information and work within the Portal is based on User Level and Role, which are described in the Tables below. Clinical Portal User Levels and Roles are listed in Table 1. User Roles may also be combined, as described in Table 2. See Table 3, "Authorized User Roles and Functions," for a functional roles matrix illustrating the ability of each assigned level to complete various functions.

2.5 **NC*Notify Roles.** Users assigned to the Clinician role in the Portal may receive access to clinical and demographic information in the Portal through NC*Notify alerts if the Participant is using version 3.0+ or later of NC*Notify.

2.6 **NC Controlled Substance Reporting System (CSRS):** Access to the NC Controlled Substance Reporting System (CSRS) via NC HealthConnex will be granted after the User has completed the CSRS enrollment process through the North Carolina Department of Health and Human Services. Enrolled Users will be assigned the appropriate CSRS role in NC HealthConnex, which will enable users to access this functionality through the NC HealthConnex portal. The CSRS roles are referenced in Table 4 below

Table 1. Clinical Portal User Levels and Roles

Level	Description	Common Examples
%HS_Clinician	This level of access is assigned to a credentialed health care provider or someone who works under a credentialed health care provider that provides patient care functions and must access clinical data. Note that the Clinician role does **not** require that the user be a physician or mid-level practitioner.	• Physician • Physician Assistant • Nurse Practitioner • Nurse • Resident or Intern • Therapist • Pharmacist • Medical Assistant • Clinical Care Coordinator
%HS_Clerical	This level of access is assigned to a user who may access the Clinical Portal to search for patients and verify demographics. This level of Authorized User may not access clinical data.	• Practice Manager • Administrator • Billing Clerk • Registration Staff •
%HS_PAAUserAdministrator	This level of access is assigned to an Authorized User who creates and maintains NC HealthConnex Clinical Portal Authorized User Accounts for their organization, including password management. This level of Authorized User may not access any patient data.	• Participant Account Administrator (PAA) • Healthcare Organization (HCO) Staff
%HS_Clinician & %HS_PAAUserAdministrator	This level of Authorized User creates and maintains NC HealthConnex Clinical Portal Authorized User accounts for their organization, including password management, and is also a health care provider or	• A clinician or health professional who requires access to patient data and who is the PAA and

	works under a health care provider to perform patient care functions. This level of Authorized User may access all the administrative and clinical functionality within the Clinical Portal.	also requires patient access.
%HS_NCNotify	This level of access is assigned to a user who *only* needs access to **view** patient notification/alerts within the NC*Notify Dashboard in the clinical portal. This level does not give permission for the user to access any other clinical data in the clinical portal	• Care Team Member • Practice Manager • PAA • Nurse • Physician
%HS_NCNotify_SSPL	This level of access is assigned to a user who maintains the NC*Notify patient panel for their organization. The user will be able to upload a patient panel within the clinical portal. This level does not give permission for the user to access any other clinical data in the clinical portal, including viewing notifications.	• Care Team Member • Practice Manager • PAA • Nurse • Physician •

Table 2. Clinical Portal User Role Combinations

%HS_Clinician & %HS_PAA User Administrator
%HS_Clinician & %HS_NCNotify
%HS_Clinician & %HS_NCNotify_SSPL
%HS_Clinician & %HS_PAA User Administrator & %HS_NCNotify
%HS_Clinician & %HS_PAA User Administrator & %HS_NCNotify & %HS_NCNotify_SSPL
%HS_Clinician & %HS_NCNotify & %HS_NCNotify_SSPL
%HS_PAA User Administrator & %HS_NCNotify
%HS_PAA User Administrator & %HS_NCNotify_SSPL
%HS_PAA User Administrator & %HS_NCNotify & %HS_NCNotify_SSPL
%HS_Clerical & %HS_NCNotify
%HS_Clerical & %HS_NCNotify_SSPL
%HS_Clerical & %HS_NCNotify & %HS_NCNotify_SSPL
%HS_Clerical & %HS_ PAA User Administrator
%HS_Clerical & %HS_ PAA User Administrator & %HS_NCNotify
%HS_Clerical & %HS_ PAA User Administrator & %HS_NCNotify_SSPL
%HS_Clerical & %HS_ PAA User Administrator & %HS_NCNotify & %HS_NCNotify_SSPL
%HS_NCNotify & %HS_NCNotify_SSPL

Table 3. Authorized User Roles and Functions

Clinical Portal Functionality	Clinician	Clerical	PAA User Admin	Clinician & PAA Admin
View Clinical Portal Home Page	X	X		X

View User Administration Home Page			X	X
Search for Patients	X	X		X
View Recent Patients	X	X		X
Break the Seal (Patient Level Access)	X			X
View Demographics	X	X		X
View Encounter History	X			X
View Allergies	X			X
View Medication History	X			X
View Problems	X			X
View Procedures	X			X
View Lab & Pathology Results	X			X
View Radiology Reports	X			X
View Clinical Documents	X			X
View Continuity of Care Documents	X			X
Access NC*Notify Notifications ***Additional enrollment steps required.***	X		X	**X**
Search CSRS ***Additional enrollment steps required.***	**X**			**X**

Table 4. CSRS Roles

Role	Description	Common Examples
%HS_CSRS_Physician	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for physicians.	• Physician
%HS_CSRS_Pharmacist	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for pharmacists.	• Pharmacist
%HS_CSRS_NursePractitioner	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for nurse practitioners.	• Nurse Practitioner
%HS_CSRS_Psychologist	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for psychologists with prescriptive authority.	• Psychologist (with prescriptive authority)
%HS_CSRS_Optometrist	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for optometrists with prescriptive authority.	• Optometrist (with prescriptive authority)
%HS_CSRS_NaturopathicPhysician	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for naturopathic physicians with prescriptive authority.	• Naturopathic Physician (with prescriptive authority)
%HS_CSRS_PhysicianAssistant	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for physician assistants with prescriptive authority.	• Physician Assistant (with prescriptive authority)
%HS_CSRS_MedicalResident	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for medical residents with prescriptive authority.	• Medical Resident (with prescriptive authority)
%HS_CSRS_MedicalIntern	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for medical interns with prescriptive authority.	• Medical Intern (with prescriptive authority)
%HS_CSRS_Dentist	This role will be used only for users who have completed the CSRS enrollment process. This role will be used for dentists.	• Dentist

2.7 Direct Secure Messaging Authorized User Authorization

2.7.1 NC HealthConnex Web DSM

a. In order to access the Direct Secure Messaging ("DSM") feature within the NC HealthConnex Portal, participants must have an active Clinical Portal account. To obtain a DSM account, the organization's Participant Account Administrator will complete the required fields in the User Management Spreadsheet and submit the request to the NC HIEA Help Desk.

b. The Participant Account Administrator or other designated point of contact will be responsible for approving additional DSM Users at each Participant organization. The NC HIEA's technology partner, SAS Institute, will process all requests for DSM Users.

2.7.2 DSM XDR

a. DSM XDR supports Direct Secure Messaging for electronic health record (EHR) and electronic medical record (EMR) systems that have integrated support for the DSM standards. In order to access DSM XDR, each Participant must complete a request form.

b. The Participant Account Administrator or other designated point of contact will be responsible for approving additional DSM XDR Authorized Users at each Participant organization.

c. NC HIEA is not responsible for managing these accounts, which are accessed through Participant's EHR or EMR systems. However, each Authorized User must have an individual account that uniquely identifies the Workforce member assigned to the account. Multiple Authorized Users or general offices or departments within a facility shall not share one XDR account that is administered by NC HIEA.

SECTION 3: NC HealthConnex and DSM User Authentication

3.1 NC HealthConnex User Authentication. User authentication assures the confidentiality of health information by requiring that the identities of all individual Authorized Users are verified when accessing NC HealthConnex. This policy sets forth the actions required for authentication when an individual attempts to access NC HealthConnex and this policy establishes standards for authentication. The NC HIEA and its Participants will have responsibilities related to authentication. The NC HIEA will utilize single-factor authentication (username and strong password) for access to NC HealthConnex.

3.1.1 Unique User Accounts. When using the NC HealthConnex through an EMR product or through the NC HealthConnex portal, each Participant must ensure that one Workforce member is assigned to one account, which uniquely identifies the specific Workforce member. **Multiple Authorized Users or general offices or departments within a Participant's organization shall not share one account to access NC HealthConnex.**

3.1.2 Portal Username Convention. NC HealthConnex portal usernames will consist of an acronym for the participating health care facility, the first name, and the last name. For example, John Smith at ABC Clinic may have the username ABC.John.Smith. If the username is identical to that of an existing user, letters or numbers may be added to differentiate usernames.

3.1.3 Portal Password Convention. An Authorized User's NC HealthConnex Portal password must be at least eight (8) characters, contain a minimum of one (1) UPPER case letter, (1) lower case letter, one (1) number, and (1) special character; and must not be identical to any of the four (4) previous passwords created by the User. An encrypted record of all users' previous passwords will be kept in order to ensure a user does not duplicate his/her previous passwords.

3.2 Portal Authentication Attempts. Authentication must be provided at every access attempt. The NC HIEA shall record all authentication access attempts.

3.2.1 If an Authorized User attempts to log in five times with an incorrect username and/or password, the Authorized User will be prompted to enter the answer to the challenge question he/she set up on first-time log in. Upon entering the correct answer to the challenge question, the Authorized User will receive an email to the email account on file with NC HealthConnex with a temporary password. If incorrect information is entered, the system will lock the Authorized User's account, and the Authorized User must contact their organization's Participant Account Administrator (PAA) to unlock the account.

3.2.2 When a User is locked out of his/her account and the recovery link is not shown on the login screen, the User should contact his/her Participant Account Administrator or the NC HIEA Help Desk via email at HIESupport@SAS.com or by phone at (919) 531-2700.

3.2.3 Portal Password Changes. Authorized Users shall change their passwords every 90 days when prompted by the NC HealthConnex Portal. Users will be reminded to change their password upon logging into the Portal, but not via a third party EMR. Access to NC HealthConnex through a third-party EMR product will not be affected by an Authorized User's password status.

3.2.4 Confidentiality of Passwords. Authorized Users of NC HealthConnex shall not share passwords with anyone for any purpose at any time. Participants shall have Participant Access Policies in place to enforce this prohibition and must take appropriate disciplinary action if this provision is violated or the confidentiality of passwords is otherwise compromised.

3.2.5 **Portal User Changes.** The Participant Account Administrator shall make request portal User account changes based on personnel changes within five (5) business days in order to ensure former Workforce members no longer have access to NC HealthConnex. This can be done in the Clinical Portal under the PAA Tools tab.

3.3 DSM User Authentication

3.3.1 **Unique Authorized User Accounts.** Whether using XDR DSM or NC HealthConnex Web DSM, each Participant must ensure each DSM account uniquely identifies the Workforce member assigned to the account. Multiple Authorized Users or general offices or departments within a facility shall not share one DSM account that is administered by NC HIEA.

3.3.2 **DSM Username Convention.** NC HealthConnex Web DSM addresses will consist of the first name of the user, the last name of the user, and the health care organization name. For example, John Smith at ABC Clinic may have the DSM account name “John.Smith@.direct.ABC.nchie.net.” If the username is identical to that of an existing Authorized User, letters or numbers may be added to differentiate usernames.

3.3.3 **DSM User Changes.** The Participant Account Administrator shall request portal User account changes based on personnel changes within five (5) business days in order to ensure former Workforce members no longer have access to NC HealthConnex.

3.4 **Confidentiality of Passwords.** XDR DSM and NC HealthConnex Web DSM Authorized Users shall not share DSM account passwords with anyone for any purpose at any time. Participants shall have Participant Access Policies in place to enforce this prohibition and must take appropriate disciplinary action if this provision is violated or if the confidentiality of passwords is otherwise compromised.

3.5 **Authentication Violation.** NC HIEA Participants are responsible for reporting to the NC HIEA suspected activity in violation of NC HIEA Policies or any activity that may cause harm to NC HealthConnex or its Participants. Reporting can be done by emailing HIEA@nc.gov or HIESupport@SAS.com. **Please do not send Personally Identifying Information or Protected Health Information via email to the NC HIEA or SAS.** Most emails sent to NC HIEA are considered public records and may be disclosed in response to a public records requests.

SECTION 4: Permitted Uses of NC HealthConnex

4.1 Permitted Uses of NC HealthConnex and Services

4.1.1 Participants and their Authorized Users are granted access to NC HealthConnex and its services solely for the performance of their roles as health care providers or in support of health care providers. Authorized Users may only access, use, and disclose information for the Permitted Purposes listed in the Participant's Participation Agreement.

4.1.2 Participants must have Participant Access Policies in place to deter unauthorized access to and use of HIE Data. These policies should include disciplinary action for breaches of PHI data or unauthorized access, use, or disclosures.

4.1.3 Examples of unauthorized access, use, or disclosure of the NC HealthConnex system, data, or NC HIEA services, absent uses permitted under the Permitted Purposes, include, but are not limited to:

a. Searching NC HealthConnex for yourself or for your family members;

b. Searching NC HealthConnex for friends or persons familiar to you if those persons are not being treated by your Participant organization;

c. Giving portal access to persons not in the Participant's Workforce;

d. Assigning Direct Secure Messaging email accounts through NC HealthConnex to persons or entities who are not in Participant's Workforce; or

e. Sharing other services or features provided by the NC HIEA with other persons, entities, or health care facilities that are not part of Participant's workforce. NC HIEA services and features include the Provider Directory, access to meaningful use registries, and all services only available to NC HIEA Full Participants.

4.2 For more information on what the Permitted Purposes for using NC HealthConnex are, please refer to your organization's executed Participation Agreement.

SECTION 5: Audit Policy

5.1 **Auditing.** The purpose of the Audit Policy is to provide ongoing monitoring of compliance with all Applicable Law, regulations, and NC HIEA Policies. The ability to execute periodic and ad hoc audits enables the NC HIEA to monitor Participants' compliance with NC HIEA contractual requirements and, if detected in the course of such monitoring, violation of legal regulatory requirements. If the NC HIEA finds that a Participant is in violation of its contract, the NC HIEA will take action to enforce the contract with the Participant. The NC HIEA is not responsible for nor obligated to monitor general legal or regulatory compliance by its Participants. However, the NC HIEA will take what it deems to be reasonable steps (e.g., typically notification of the Participant) if such violations are detected during the course of an audit. The NC HIEA and its Participants will have responsibilities related to an audit.

5.1.1 The NC HIEA 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 NC HealthConnex access and the use and disclosure of Protected Health Information available through NC HealthConnex. Entry will be immutable (unchanging and unchangeable) in content.

5.1.2 The NC HIEA will maintain an active audit trail for at least six years.

5.1.3 Internal audits within Participants' own organizations should also be performed in order to ensure patient information is kept secure.

5.1.4 **Break the Seal.** A separate audit log will be stored by the NC HIEA for "Break the Seal" instances where an Authorized User is required to gain further information on a patient that does not yet have a clinical relationship established to a participating provider within NC HealthConnex. In addition, certain case management entities may be subject to a user-by-user audit to determine proper usage of the system.

5.2 **Quarterly Audit.** The NC HIEA will perform audits at least quarterly to maintain updated Authorized User lists for each practice and to ensure the activity of users is legitimate. A report of active Users is updated quarterly and made available on the Participant Account Administrator's homepage within NC HealthConnex. The Participation Account Administrator must request updates on the then-current make up of staff to the NC HealthConnex Help Desk and click the Attest Button within the NC HealthConnex portal account to confirm an accurate record of their users within ten (10) business days. Failure to respond to multiple quarterly audits will result in the entire Participant organization or participating entity losing access to the Clinical Portal and other NC HealthConnex features.

SECTION 6: Required Equipment and Software; Security

6.1 Software and Equipment.

6.1.1 Each Participant is responsible for procuring or having access to all equipment and software necessary to submit data to the NC HIEA, to access the NC HealthConnex portal, and to Transact Messages over the eHealth Exchange when needed. All computers and electronic devices owned, leased, or operated by Participants must be properly configured, including, but not limited to, the base workstation operating system, web browser, and internet connectivity.

6.1.2 Pursuant to HIPAA and the NC HIEA Participation Agreements, each Participant shall use and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of HIE Data and to prevent the acquisition, access, disclosure, or use of HIE Data through NC HealthConnex other than for Permitted Purposes.

6.1.3 Authorized Users should not leave a computer or laptop unattended when logged into NC HealthConnex, such that unauthorized individuals might inappropriately access the NC HealthConnex platform and information contained therein.

a. All desktop and laptop computers with access to NC HealthConnex, when not monitored directly, must have the following controls performed:

i. Authorized User(s) logged out of the system;

ii. Password-protected screen saver; or

iii. System shutdown, if other options are not available.

b. All mobile communication devices (e.g. smart phones and tablets) with access to NC HealthConnex, when not monitored directly, must have the following controls performed:

i. Authorized User(s) logged out of the system;

ii. Mobile device to lockout after five (5) minutes of non-use; or

iii. System shutdown, if other options are not available.

6.1.4 For supported web browsers and mobile device requirements, please see the NC HealthConnex User Guide.

6.2 Malicious Software. Each Participant shall ensure that its security controls meet applicable state or federal requirements and standards so as to not introduce any viruses, worms, unauthorized cookies, Trojans, malware, or other malicious software that could damage, destroy, make inoperable, or cause improper access to the Participants’ system, HIE Data, eHealth Exchange Messages, or any system or service connected to NC HealthConnex.

User Access Policy Changes

Location or Section	Change Made	Date
Entire Policy Document	Removed old headers and footers, added in NC HealthConnex Logo	6/18/2019
Introduction	Removed statutory deadlines; included reference to health plan participation	6/18/2019
Section 1: Definitions	Added definition of Clinical Portal; amended definition of Authorized User	6/18/2019
Section 2: User Authorization & Access Roles	Language on emergency opt out exception removed; portal user and Direct secure messaging account information amended based on upgrade to InterSystems; added information on user access to the NC Controlled Substance Reporting System	6/18/2019
Section 3: NC HealthConnex and DSM Use Authentication	Amended portal and DSM user account management information based on upgrade to InterSystems; amended SAS Help Desk phone number	6/18/2019
Section 4: Auditing Policy	Added language regarding user account suspension if participant does not respond to multiple quarterly audits; removed requirement for participants to notify NC HIEA of personnel changes	6/18/2019
Section 5: Required Equipment and Software; Security	Renamed the user guide to the NC HealthConnex User Guide	6/18/2019
Entire Policy Document	Non-substantive edits to enhance readability; updates to align provisions with defined terms.	4/5/2021
Introduction	Restated legislative history; revised statement about amendment to Policies; new effective date.	4/5/2012
Section 1: Definitions	Added references to “Portal’ and “PAA”	4/5/2021
Section 2: User Authorization & Access Roles	Non-substantive revisions added for clarity; moved subsection concerning the NC Controlled Substance Reporting System; provisions added concerning Unauthorized Access and consequences for inappropriate use of NC HealthConnex; provisions added concerning NC*Notify; provisions added concerning User Roles, including “combined” roles and roles for NC*Notify.	4/5/2021
Section 3: NC HealthConnex and DSM Use Authentication	Clarifying edits to enhance readability; remove duplicative statement concerning NC HIEA responsibility for User Authentication policy; strengthen provision concerning password confidentiality.	4/5/2021

Section 4: Permitted Uses of NC Health Connex	Clarifying edits added regarding unauthorized access and use of NC HealthConnex.	4/5/2021
Section 5: Audit Policy	Clarifying edits to describe certain responsibilities Participants and the NC HIEA have with respect to the Audit Policy, including revisions to Quarterly Audit to reflect updated practice; provision deleted concerning NC HIEA outreach.	4/5/2021
Section 6: Required Equipment and Software; Security	Clarifying edits to enhance readability and describe requirements.	