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 NC HIEA was created by the NC General Assembly in N.C.G.S. 90-414.1, et seq., and NC Session Law 2015-241 §§12A.4 and 12A.5. The NC HIEA has been directed to establish an electronic statewide 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. The goal of NC HIEA 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. To support that goal, the legislation requires all Medicaid providers to be connected to NC HealthConnex by February 1, 2018, and all other entities that receive state funds for the provision of health services, including managed care organizations and local management entities, to be connected by June 1, 2018.

In addition, the Medicaid Transformation bill requires all prepaid health plans, Medicaid providers, and NC Health Choice providers to submit data to NC HealthConnex in order to ensure effective systems and connectivity to support clinical coordination of care, the exchange of information, and the availability of data to the NC Department of Health and Human Services and the Division of Health Benefits to manage the Medicaid and NC Health Choice programs for the state.

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 agree to 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. These Policies may be amended from time to time by the NC HIEA staff in consultation with the NC HIEA Advisory Board. Definitions include references to laws or regulations as appropriate to illustrate the context and intent of this Policy.

These Policies are effective as of November 1, 2016.
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 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 provided therein.

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

1.6 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.

1.7 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.

1.8 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 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.

1.11 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.

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

1.13 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.

1.14 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.

1.15 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.
1.16 **Participant Account Administrator** 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.

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

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

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

1.20 **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.

1.21 **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 will create a list of universal access roles based on the level of information necessary for care. Each Participant Account Administrator 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 a patient’s information will only be 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 providers can establish a relationship with a patient for treatment purposes if the patient has not opted out of NC HealthConnex. If an individual has opted out of NC HealthConnex, only a Level 6 NC HealthConnex Administrator or Privacy Officer has the ability to rescind that individual’s opt out in order for a provider to access the patient record in the event of an emergency.

2.2 Portal User Authorization. This policy sets forth the minimum requirements for Authorized Users of the NC HealthConnex 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. At present, authorization of access to health information is limited to treatment, payment for treatment and health care operations, and the Permitted Purposes provided in the NC HIEA Participation Agreement. New user accounts are created with the approval of the Participant Account Administrator.

   a. Role-based Access: The NC HIEA, through SAS Institute, its technology vendor, will assign at least one Participant Authorized User to the “Level 5 Participant Account Administrator” role at each Participant’s organization. This Participant Account Administrator will have the authority to create and maintain Authorized User accounts for other users in the practice. 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 creation and management of users who access NC HealthConnex. No user will be authorized to access NC HealthConnex unless the Participant Account Administrator and/or authorized designee 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 in giving Workforce members access to NC HealthConnex and all NC HealthConnex Services, including Direct Secure Messaging. Participant Account Administrators are not authorized to give user credentials to persons or entities that are not Participating Entities under control of the Participant organization or to persons not included in Participant’s Workforce. 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.
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 his role within the Participant organization.

<table>
<thead>
<tr>
<th>Level</th>
<th>Title/Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Primary Provider</td>
<td>Physician</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nurse Practitioner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resident</td>
</tr>
<tr>
<td>Level 2</td>
<td>Secondary Provider</td>
<td>Nurse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Therapist</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pharmacist</td>
</tr>
<tr>
<td>Level 3</td>
<td>Care Support</td>
<td>Unit Clerk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medical Assistant</td>
</tr>
<tr>
<td>Level 4</td>
<td>Front Desk Staff</td>
<td>Billing Clerk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medical Assistant II</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Registration Staff</td>
</tr>
<tr>
<td>Level 5</td>
<td>Participant Account Administrator</td>
<td>User Account Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Healthcare Organization (HCO) Staff</td>
</tr>
</tbody>
</table>
Level 6

User account administrators are responsible for creating, changing and deleting NC HealthConnex end user accounts as well as Communicate Webmail accounts (if applicable) including password management. They are also responsible for creating and maintaining EMPI Administrator accounts whereas Organization User Account Administrators can manage users only within their own organization.

Privacy officers are responsible for the monitoring and auditing of NC HealthConnex access as well as manually updating patient consent (opt-in/out) status.

NC HealthConnex Administrator or Privacy Officer

2.4 **Functions Based on User Level.** The ability of Authorized Users to view certain types of clinical information and work within the portal is based on which level their role falls under. Below is a functional roles matrix illustrating the ability of each assigned level to complete various functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
<th>Level 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Clinical Homepage</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Front Desk Homepage</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search for Patients</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View Recent Patients</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Break the Privacy Seal (Patient Level Access)</td>
<td>X*</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>*Sensitive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Demographics</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>View Encounter History</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View Allergies</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Medication History</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Problems</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Procedures</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Lab &amp; Pathology Results</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Radiology Reports</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NC HealthConnex Administrator

Compliance Officer
Privacy & Security Officer
2.5 Direct Secure Messaging User Authorization

2.5.1 Communicate Webmail User Authorization

a. In order to access the Direct Secure Messaging ("DSM") feature within the NC HealthConnex portal called Communicate Webmail, each Participant organization must complete a DSM Web Application listing all Authorized Users who will be using Communicate Webmail. The Participant must also designate a point of contact, preferably the Participant Account Administrator, and complete a Declaration of Identity. This Declaration of Identity must be validated by DigiCert, Inc., the organization that issues digital certificates to Communicate Authorized Users.

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

2.5.2 Communicate Direct XDR

a. Communicate Direct 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 Communicate Direct XDR, each Participant must complete a Communicate Direct XDR Health Care Organization Account Request Form.

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

c. NC HIEA is not responsible for managing these accounts as they are accessed through Participant’s EHR or EMR systems. However, each 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 Use 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 attempting to access NC HealthConnex and to establish standards for authentication. The NC HIEA and its Participants will have responsibilities related to authentication. The NC HIEA will make this policy known through participant outreach and education, and enforce through the Participation Agreement and Business Associate Agreement. The NC HIEA will utilize single-factor authentication (user name 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 User Name Convention.** NC HealthConnex portal user names 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 user name 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) UPPERCASE letter, (1) lowercase letter, one (1) number, and (1) special character; and must not be identical to any of the twenty-four (24) 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 their previous passwords.

3.1.4 **Portal Authentication Attempts.** Authentication must be provided at every access attempt. The NC HIEA shall record all authentication access attempts. After three (3) consecutive failed log-in attempts, a user will be locked out. The lock-out will last for 30 minutes. Authorized Users can utilize the Forgot My Password link to answer a secret question if this function has been previously configured on the My Details screen. If this link is not shown on your login screen and you are locked out of your account, please contact your Participant Account Administrator or the SAS Help Desk via email at HIESupport@SAS.com or by phone at (919) 677-8008 or 1-800-727-0025.

3.1.5 **Portal Password Changes.** Authorized Users will have to 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.

3.1.6 **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.

3.1.7 **Portal Authentication Data & User Changes.** The NC HIEA shall ensure authentication data is secure at the time it is entered and is administered safely. The Participant shall inform the NC HIEA of Participant Workforce personnel changes within five (5) business days in order for the NC HIEA to change or terminate the former Workforce member’s access to NC HealthConnex.
3.2 DSM User Authentication

3.2.1 Unique Authorized User Accounts. Whether using XDR Direct Communicate or Communicate Webmail through the NC HealthConnex portal, 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.

3.2.2 DSM User Name Convention. NC HealthConnex Communicate 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 user name is identical to that of an existing user, letters or numbers may be added to differentiate usernames.

3.2.3 Communicate Webmail Password Convention. An Authorized User’s Communicate Webmail 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 twenty-four (24) previous passwords created by the User. It also cannot contain any part of your login name. An encrypted record of all users’ previous passwords will be kept in order to ensure a user does not duplicate a previous password.

3.2.4 Communicate Webmail Authentication Attempts. Authentication must be provided at every access attempt. The NC HIEA shall record all authentication access attempts. After three (3) consecutive failed log-in attempts, a user will be locked out. The lock-out will last for 30 minutes. Authorized Users can utilize the Forgot My Password link to answer a secret question if it has been previously configured on the My Details screen. If this link is not shown on your login screen and you are locked out of your Communicate Webmail account, please contact your Participant Account Administrator or the SAS Help Desk via email at HIESupport@sas.com or by phone at (919) 677-8008 or 1-800-727-0025.

3.2.5 Communicate Webmail Password Changes. A Communicate Webmail Authorized User will have to change his password every 90 days when prompted by NC HealthConnex.

3.2.6 DSM User Changes. The Participant shall inform the NC HIEA of Participant Workforce member changes within five (5) business days in order for the NC HIEA to change or terminate the former Workforce member’s access to DSM.

3.3 Confidentiality of Passwords. Direct Communicate XDR and Communicate Webmail 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.

3.4 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 Personal Health Information via email to the NC HIEA or SAS.
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 against 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 services or features provided by the NC HIEA with persons, entities, or health care facilities that are not Participants of NC HealthConnex. NC HIEA services and features include the Provider Directory, access to meaningful use registries, and all services only available to NC HIEA Participants.

4.2 For more information on what the Permitted Purposes for using NC HealthConnex are, please refer to the Participation Agreement that your organization has executed.
SECTION 5: Auditing 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 gives the NC HIEA the ability to monitor participating providers’ compliance with NC HIEA contractual requirements and, if detected in the course of such monitoring, violation of legal regulatory requirements. If the NC HIEA does find that a participating provider is in violation of its contract, NC HIEA will take prompt 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, 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 audit. The NC HIEA will make this policy known through participation outreach and education and enforce it through the Participation Agreement and Business Associate Agreement. 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 personal health information available through NC HealthConnex. Entry will be immutable (unchanging and unchangeable) in content.

5.1.1 The NC HIEA will maintain an active audit trail for at least six years. Provider audits should be ongoing in order to ensure patient information is kept secure.

5.1.2 Break the seal. A separate audit log will be stored for “Break the Seal” 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 NC HealthConnex. In addition, certain case management entities will be subject to a user-by-user audit to determine proper usage of the system.

5.2 Quarterly Physician Practice Audit. An audit will be performed at least quarterly to maintain updated user lists for each practice. A report of active users is run for each practice and sent to the Participant Account Administrator for confirmation. The Participation Account Administrator must provide updates on the then current make up of staff and sign the report confirming an accurate record of their users within ten (10) business days. If there are changes noted, the NC HIEA will implement those changes and terminate access for employees no longer working with the Participant.

5.3 Notification to NC HIEA of Changes Regarding Authorized Users. Participants must notify the NC HIEA in writing if an employee who was an Authorized User of NC HealthConnex is no longer working for the Participant. Participants must also notify the NC HIEA if an Authorized User has changed roles within the health care facility as this may affect the level of access the Authorized User must occupy. The notification must be sent to the NC HIEA within five (5) business days of the change in employment status via email to HIEA@NC.Gov or by mail to the following address:

NC Health Information Exchange Authority
4101 Mail Service Center
Raleigh, NC 27699-4101
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 or leased by Participants must be properly configured, including, but not limited to, the base workstation operating system, web browser, and internet connectivity.

6.1.2 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 or as required by Applicable Law.

6.1.3 Authorized Users must not leave a computer or laptop unattended when logged into NC HealthConnex, such that unauthorized personnel might use the computer and account to access the information contained in NC HealthConnex.

   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 HIEA Primary Provider User Guide.

6.2 Malicious Software. Each Participant must ensure that their security controls meet applicable or federal 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.