Connecting People for Better Health

# Connie HIE Administrator Responsibilities

- **Lock and terminate authorized user accounts as soon as staff leave.** This ensures staff members are no longer able to log in to Connie and access clinical information under your organization's account. You are responsible for managing your Connie user list, including keeping it updated and ensuring proper use of the system.

- **Register new staff members with a Connie user account.** As an administrator, you can add employees for authorized access.

- **Conduct a monthly user audit**. Make it a best practice to perform a monthly user audit and make sure that accounts are up to date. **All user accounts need to be validated every 90 days or user access will be automatically suspended.**

- **Keep Connie updated of any general practice changes**, such as change of address, phone number, fax, or email. Connie Account Managers conduct periodic touchpoints to offer support, check in, and share any Connie updates since the last touch base. Also, your Account Manager may email important communications relevant to your organization, so please make sure Connie has up-to-date contact and location information.

- **Report any potential issues.** If you experience any issues with your Connie user account or services, please let Connie Support know as soon as possible. For technical assistance, contact 866-987-5514 or help@conniect.org

- **Alert your Connie Account Manager if you or your organization would like to receive additional training materials.** Connie will reconnect with you several times a year, but feel free to reach out if you need additional support of support documents!

# Confidentiality and Non-Disclosure Best Practices

As a HIPAA covered entity or business associate, you should be aware of the rules around HIPAA. This includes the responsibility you, and your users, have to follow best practices in accessing and using patient health information and other confidential information you may have access to using the Connie services. Information that may be considered confidential can include, but is not limited to patient identifiable information, employee identifiable information, intellectual property, financially non-public information, contractual information, and information of a competitive advantage nature.

Confidentiality and integrity of information are to be preserved and its availability maintained. The value and sensitivity of information is protected by law and by the Connie data sharing agreement. The intent of these laws and Connie policies is to assure that confidential information will remain confidential through its use.

Misuse of Connie includes accessing or viewing information on a relative or acquaintance with whom no clinical relationship or need to know exists – i.e., parent, sibling, child (including children under 18 years of age), spouse, significant other, co-worker, neighbor, etc.

As a condition to receiving a unique user log-in identification and password, or credentials, and authorized access to Connie, and/or being granted authorization to access any form of confidential information, users agree to comply with the Connie policies and procedures. Users should be aware and informed about the following best practices:

- User names and passwords should be regarded as equivalent to a legal signature. Users should not disclose their passwords to anyone or allow anyone to access the system using their login credentials.
- Users are responsible and accountable for all data accessed and all entries made under their login credentials, whether those actions were due to their own intentional or negligent act or omission.
- Users should not ask for or attempt to learn or use another authorized user's log-in credentials.
- Users should not access Connie using any login credentials other than their own assigned by their HIE Admin.
- Users should immediately reach out to their HIE Admin or Connie Support if they have any reason to suspect that the confidentiality of their login credentials has been compromised.
- Users should never leave their workstation unattended while logged in to Connie.
- Users must comply with all policies and procedures and other rules of Connie relating to confidentiality of information and login credentials.
- Any data available to users through Connie services should be treated as confidential information as defined by HIPAA.
- Users should know that their use of Connie services will be routinely monitored to ensure compliance with Connie policies and procedures.

- Users should not access, view, or request information on anyone with whom they do not have a clinical relationship or a need to know in order to perform their official job responsibilities.
- Users should not disclose any confidential information unless required to do so in the official capacity of their employment or contract. They must also understand that they have no right or ownership interest in any confidential information accessed through Connie.
- Users should not disclose protected health information or other information that is considered proprietary, sensitive, or confidential unless there is a legitimate need.
- Users should limit distribution of confidential information only to parties with a legitimate need in performance of their organization's mission.
- Users should be aware that disclosure of confidential information is prohibited indefinitely, even after termination of their employment or business relationship, unless specifically waived in writing by the authorized party.
- Users must not use the information they access through Connie services in any way that is detrimental to the organization and will keep all such information confidential.
- Users must also understand that inappropriate access may be a criminal offense that could be subject to prosecution by the State of Connecticut.
- Users need to be aware that their continued use of Connie and Connie services rests on their compliance with HIPAA and local, state, and federal laws governing confidentiality and privacy. Violation of those laws can subject them, or their employer, to disciplinary action including loss of privileges and termination of contract. In very serious cases, users or their employer, can be subject to legal action or other remedies available to Connie.