CONNIE HIE

OPERATING POLICIES AND PROCEDURES

VERSION 1.0
DATE: NOVEMBER 2022

Connie

Contents

Background

These Operating Policies and Procedures contain specific terms and conditions of operation and use of the Entity Services ("Connie Services"), as well as other terms or requirements relating to the Connie Services as are specified in the Qualified Data Sharing Organization Agreement (QDSOA), the Simple Data Sharing Organization Agreement (SDSOA), or the State of Connecticut Personal Service Agreement (PSA), collectively the "Agreements". These Operating Policies and Procedures are consistent with, or supplement or implement the provisions of, the Agreements. In the event of a conflict between a provision of the Agreements and a provision of these Operating Policies and Procedures, the provision of the Agreements will govern. The Operating Policies and Procedures may be amended from time-to-time in accordance with Section 3.7 of the QDSOA, Section 3.9 of the SDSOA, and Section C.4 of the PSA.

Participant acknowledges that Participant is responsible for reviewing the Operating Policies and Procedures when provided by Connie and for monitoring communication from Connie on a regular basis for, among other things, amendments to the Operating Policies and Procedures or notices relating to such amendments made in accordance with the applicable section of the Agreements. Unless otherwise noted, capitalized terms contained herein have the meaning given to them in the Agreements.

Participant Users

Participants may provide access to Connie Services to their employees or other individuals who require access as part of their job function ("Participant Users"). Participant Users may have Connie Services access rights at multiple participant locations or organizations based on their employment. If such a Participant User chooses to access the Connie Services via the web-based portal application made available through Connie, a username and password will be assigned to that user for each Participant.

Participants must have enforceable agreements with each of their Participant Users. Agreements may take the form of written policies and procedures of the participant, as long as such policies and procedures constitute an enforceable agreement with users. Participants must require that all of their Participant Users comply with applicable laws; clauses in the Agreements directly applicable to Participant Users; and this Connie Operating Policies and Procedures. If a Participant User is in violation of any of these requirements, Participant must immediately notify Connie, and Connie may suspend or terminate the Participant User, in its reasonable discretion.

1.1 Change in Participant User's Job Status or Role

Participants are responsible for promptly informing Connie (i) when the job status or role of a Participant User within their organization has changed, if such change affects their access rights to the Connie Services and (ii) for changing the role of a Participant User if access is obtained through a third-party electronic health record (EHR). If a Participant User is being terminated from a Participant, the Participant must inform Connie of this termination within five (5) business days, and prior to actual termination if at all possible. Connie will terminate the Participant User's account immediately upon notification of termination of employment from the respective Participant. Participants accessing the Connie Services through third- party EHRs, via SSO/SAML, will be responsible for terminating access through this EHR for the terminated Participant User at the time of termination. However, Participants must still notify Connie within five (5) business days so that Connie can terminate access to other Connie tools and services that are not accessed via SSO/SAML, including but not limited to Direct messaging.

1.2 Training

Connie will make training available through online tools such as onboarding webinars, in addition to other training materials, as appropriate. Participant will be responsible for training individual users on data consumption, Connie policies, and in accordance with the Agreements and HIPAA Addendum, including the creation and dissemination of any necessary training provided by Connie (*See Section 8.3. Maintenance*). If additional training is necessary as a result of system updates, Connie will provide training resources and inform Participant of the changes, and each Participant will then be responsible for training all of its Participant Users.

2. User Name and Passwords

Connie will utilize security-industry standards for authenticating user access to Connie Services and tools. Connie and Participants must ensure that each Participant User is assigned a unique username and password and that multi factor authentication (MFA) is enabled on each account to access the Connie Services and tools.

2.1 Password Convention

Connie password requirements differ across the tools and services. Connie will communicate requirements as needed for each Connie Service and tool. Participant User passwords will expire every 90 days, requiring that each Participant User to select a new password at that time. Password history settings will be enforced to ensure that a Participant User does not duplicate a password used previously.

2.2 Lock Outs and Password Resets

Participant Users will be able to reset their password using answers to the challenge questions set during initial login for the Portal. After five (5) consecutive failed log-in attempts, a Participant User will be locked out of the Connie Service or tool. In order to get his/her account unlocked, a Participant User must call the Connie Customer Support desk directly at 1-866-987-5514. Participant Users whose accounts do not have any activity for a duration of ninety (90) days or longer will be automatically locked out of their account. HIE Admins can unlock suspended accounts as long as the account has not been suspended for longer than 120 days. If an account has been suspended for 120 days or longer, Participant Users must call Connie to get their account unlocked. Participant Users not using single sign on must be verified every 90 days by the HIE Admin of the Participant.

3. User Access Policies

All Participants are required to develop, or have in place, written requirements that govern Participant's and Participant Users' access to information systems and use of protected health information. Such policies should be consistent with the permitted purposes in the Agreements and these Operating Policies and Procedures and should be made available to Connie upon request. Participants must appoint an authorized individual to implement and ensure compliance with all policies related to Connie Participant Users. The authorized individual will be responsible for implementing a policy that appropriately grants Participant Users access to clinical data on behalf of the Participant. This authorized individual may also act as the designated point of contact for Connie correspondence and user verification and updates as described in Section 8.

3.1 Minimum Necessary

Participant Users agree to view, use, and/or disclose the minimum amount of information necessary for the purpose of such use. Participant Users should only have access to the minimum amount of information required to perform their job function. Minimum necessary does not apply to use of data for treatment or purposes required by law. It is the Participant's obligation to ensure the appropriate use of Connie Services by Participant and Participant Users.

3.2 Data Misuse

Health information available through Connie is to be accessed, viewed, and used only by Connie Participants and authorized Participant Users, and only for permitted purposes. Connie uses a privacy tool for additional monitoring of all Participant User activities regarding protected health information access to ensure all provisioned accounts are being used appropriately and to protect the confidentiality of protected health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of Connie Services by Participant and Participant Users. Any actual or suspected misuse of protected health information in connection with Connie Services must be reported to Connie as soon as discovered. The actual or suspected misuse of protected health information will be investigated by Connie and the Participant. Connie will notify privacy and security officers of all impacted parties at the conclusion of such investigations, if it is determined that a misuse of protected health information has occurred. As appropriate, Connie and/or the Participant will also take actions necessary to remedy the misuse of data. These actions may include, but are not limited to, suspension and/or modification of access privileges for a Participant or Participant User(s).

3.3 Participant Procedures for Non-Compliance

In accordance with the Agreements, each Participant should implement procedures to mitigate and deter misuse and issue appropriate consequences to hold Participant Users accountable for misuse of data obtained when accessing protected health information through the Connie Services. As applicable, procedures in place for use of other health information systems may be leveraged to satisfy the requirements of this Section 3.3.

3.4 PO Participants

Participants may have relationships with unaffiliated third parties whereby that third party sends, receives, finds, or uses data via the Participant with Connie Services ("PO Participants"). Participant is responsible for having valid and enforceable agreements with each of its PO Participants that require the PO Participant to, at a minimum: (i) comply with all Applicable Laws and Standards; (ii) comply with the terms of the Agreement as applicable including but not limited to protecting the privacy and security of any data to which it has access; (iii) refrain from disclosing to any other person any passwords or other access credentials issued to the PO Participant by the PO; and (iv) comply with the relevant sections of these Operating Policies and Procedures, including, but not limited to Sections 3.1, 3.2, and 3.3, as applicable.

4. Patient Access and Rights

4.1 Accounting of Disclosure Requests

Patients can request an accounting of disclosure of a Participant's access of the patient's information. Connie requires the patient request include first name, last name, date of birth, address, and a copy of a government-issued photo ID. Patients may access the Accounting of Disclosure Request Form on Connie's website at www.conniect.org/for-patients/privacy-and-security-controls. Completed forms can be emailed to disclosures@conniect.org. Patients may also contact Connie Customer Support at (866) 987-5514.

4.2 Opting Out of Connie Services

Unless otherwise required by Applicable Law, Connie's default patient consent policy is opt-out. This means that a patient must proactively, and explicitly, declare their desire to opt out of the exchange. Opting out means that a patient's health information will no longer be returned as the result of a query or sent as an encounter notification. Opting out does not apply to point-to-point secure messaging (e.g., Direct messaging). For example, if a primary care physician uses Direct messaging to communicate with a specialty physician about a patient's care, the communication will not be available to other physicians who query the exchange. It also does not apply to any state-mandated program that Connie facilitates through our technology, such as the Prescription Monitoring Program or public health reportable conditions.

The opting out of patients will be handled by Connie. It is the Participant's responsibility to adequately educate patients on the opt-out process and to ensure that its Notice of Privacy Practices is updated accordingly, if and to the extent necessary. Patients can opt out by completing a paper form and mailing or faxing it to Connie, calling a toll-free number (1-866-987-5514), or via online form submission (conniect.org/for-patients/opt-out). There may be a period of up to five (5) business days after Connie's receipt before the opt-out is effective, meaning that patient data may be available for query during this interim time after the opt-out has been submitted. Patients are allowed to opt back into the exchange at any time, but patient data may have been deleted during the time the opt-out was in effect.

4.3 Access to Health Information

Available Information and Methods for Access

As discussed below, patient access is a Permitted Purpose and is required, in most cases, under Applicable Law. Patients can find the types of information Connie stores as part of its routine operations on the Connie website. Connie will facilitate multiple methods for patient information access, including through third party applications and accessing information directly from Connie.

Access to Information for Minors

State or Federal law may prohibit health care providers from disclosing certain health related information about a minor patient to anyone, including parents, without the express consent of the minor. It is technically infeasible for Connie to segment or remove data from encounters or clinical documents in order to avoid disclosing specific types of information that Applicable Law prohibits being disclosed. At this time, Connie is not able to make available any information for individuals aged 12-17. Parents or legal guardians who are able to demonstrate their custodial relationship may have access to information for their children aged 0-11.

Support and Education

Connie will make available educational materials about best practices and methods for patients accessing their information, including privacy and security risks associated with certain methods or vendors. In addition, the materials will remind patients that their healthcare providers will likely have more robust information and are the appropriate contact if they have questions or concerns with the information shared. The Connie Customer Support team will answer patient questions about how to access their Connie information, but patients who have questions about their information will be directed to the health care provider who shared or created the information.

5. Permitted Purposes

Participants and Participant Users may access and use data through Connie Services for only Permitted Purposes. Current Permitted Purposes for data use are listed below:

1. For Treatment, Payment, and Healthcare operations, as those terms are defined in the Health Insurance and Portability and Accountability Act of 1996 (HIPAA), and except as set forth below.
2. For public health activities as permitted or required by Applicable Law and consistent with the mission of Connie to advance the health and wellness of patients.
3. For participation in federal programs, such as Medicare Access and CHIP Reauthorization Act (MACRA) Quality Payment Program (QPP), including Merit-Based Incentive Payment System (MIPS), and the Medicare Shared Savings Program (MSSP).
4. For transacting with External HIEs, including the eHealth Exchange, in accordance with the applicable use case.
5. For responding to requests for individual access in accordance with Section 4.
6. All other allowed purposes as determined by Connie to be required or permitted under the Applicable Law.

Permitted Purposes may be expanded or restricted through use cases. The use cases are approved and amended by the applicable Committee before their incorporation into a Permitted Purpose.

Connie may add Permitted Purposes according to the Agreements.

6. Participating Data Providers

Participants must complete testing and other onboarding activities prior to going live with connectivity to Connie. These testing and onboarding activities are tailored to the type of data being provided and accessed and typically include a patient or member panel. Connie communicates these requirements during the onboarding process. Participants should notify Connie of any changes prior to system changes or upgrades being made. Data validation should be completed by comparing the data in Connie's system to that in the Participant's source system. Connie will provide guidance on testing, but it is the Participant's responsibility to execute a complete test plan in accordance with their own testing policies and procedures. Following successful completion of participant testing, Participants must confirm that they are ready to go live.

6.1 Data Contributors

Participants will make data available that are necessary to engage Connie Services. For each Participant, information made available to the Connie Services will be subject to appropriateness and technical readiness. For a Participant to be connected to and remain connected to Connie Services, it must submit at least one defined data type. Contribution of data must occur over a secure connection configured by Connie and the Participant.

6.2 Sensitive Health Information

Participants are responsible for complying with Applicable Laws and for filtering any information that must not be disclosed to or through Connie. Data contributors of Participating Organizations must refrain from sending certain sensitive health information, including substance use disorder treatment, and may refrain from sending other sensitive health information including, but not limited to, psychiatric related services, and HIV-related information.

7. Data Retention and Reuse

Connie will retain disclosure data for a minimum period of seven (7) years, as required by Applicable Law, in order to maintain an auditable history of each transaction through the Connie Services.

Connie may allow access or otherwise release data from the Connie Services for public health reporting or in other civil, criminal, or crisis-related matters when compelled to provide that data by a lawful order, legal process, or other requirement of law. Each such request for data will be vetted to ensure the request is legal and appropriate. Connie will not release any personal health information to a Participant or a Participant User for reasons that are not related to the Permitted Purposes.

7.1 Data Consumption

A Participant can contribute and or consume data either via the Connie Services or through a third-party EHR. The hardware and software requirements for the Connie Services depend on the means a Participant is using to contribute or consume data.

7.2 Return of Data

If a Participant terminates access to the Connie Services in accordance with the Agreements, Connie will disable that Participant's data feeds and terminate the Participant's ability to access the Connie Services in accordance with the Agreements. All data that has been incorporated into a provider's EHR system prior to Participant termination will continue to be the property of that provider. Additionally, and consistent with the Agreements, Connie or Participant may retain one copy of the other's Confidential Information to the extent reasonably necessary to document matters relating to the Agreements, for legal or insurance reasons, or for similar business or operational purposes, provided that the restrictions on Confidential Information in the Agreements continue to apply to the retained copy and the retained Confidential Information is returned, deleted, or destroyed when the purpose of the retention has been fulfilled.

8. Systems Operations

8.1 Hardware and Software

Connie Services are made up of a combination of commercial, off-the-shelf applications (COTS) and custom developed applications. Connie makes data available through two core service areas:

1. Point of Care: Clinical Information
2. Care Coordination: Encounter Notifications

8.2 Availability and Network Monitoring

Connie Services are monitored continuously by Connie and/or third parties. Connie and its partners and vendors maintain agreements that provide for at least 99.7% uptime per calendar month, not including scheduled downtime. Connie commits to 99.9% of messages being delivered within 24 hours of receipt of admission, discharge, or transfer messages from supplying Participant. For each calendar year, scheduled hardware, software, and communications maintenance shall not exceed an average of 8 hours per calendar month. All scheduled maintenance will be carried out on dates and at times authorized by Connie with at least three (3) business days' notice provided by Connie or vendor to all participants via e-mail or other electronic method such as the Connie web page.

In the event of unexpected downtime, Connie will provide notifications to Participants via e-mail or other electronic method such as the Connie web page. Depending on the severity level of the problem, initial notification to Participants will occur between four (4) hours and three (3) business days after discovery of the problem. Updates will occur, via the same methods, every eight (8) business hours to every three (3) business days, depending on the severity level until notification of resolution.

8.3 Maintenance

Participants will be required to provide at least one, but preferably two, points of support contact information to Connie. Participant support staff will be expected to assist with issues surrounding on-going training, master patient index (MPI) administration, data quality, system upgrades and downtime, and privacy and security issues.

Participants that are acting as consumers of data will be required to provide at least one, but preferably two points of contact, known as HIE administrators for Connie Services. This administrator will be responsible for the maintenance of user profiles, including providing all necessary information to Connie for adding users, deleting users, and assigning or changing user roles. The Administrator must notify Connie immediately if a user's employment at the organization has been terminated or if his or her functional role has changed. This notification can be done either using the self-service HIE Admin Tool (recommended) or an email to help@conniect.org. The administrator will also be responsible for attesting to the user identity verification and checking that users have completed all necessary policy training prior to obtaining access to the Connie Services and for monitoring the general use and operations of the Connie Services.

8.4 Implementation Support

Connie and its HIE vendor(s) will make available the following implementation services (collectively, “Implementation Services”) to the Participant:

- Establish environments (test and production) for secure transactions;
- Configure environments based on Connie Operating Policies and Procedures regarding privacy, security, and consent;
- Conduct planning and decision sessions;
- Jointly document transaction types;
- Jointly document data conversion and mapping requirements;
- Establish real-time notifications, if applicable;
- Test and validate real-time notification, if applicable;
- Establish batch transaction, if applicable; and
- Test and validate batch transactions, if applicable.

8.5 Operations Support

Connie will make available the following operational support to the Participant:

- At least daily backups of the production environment;
- Transaction logs of all database updates that occur between daily backups;
- Periodic performance management;
- Disaster Recovery as required in the event of a catastrophic failure of the primary production site location using an alternate recovery site;
- Maintain Datasets (e.g., authorized users) with data supplied by Connie or Participant; and
- Support Participant’s periodic reconciliation of the Encounter Notification Services (ENS) and claims-based encounter information.

9. Support

Connie offers Participants technical support to respond to technical problems, including support for test and production environments. The technical support can be reached at help@conniect.org or 1-866-987-5514. Connie Customer Support uses a trouble ticket logging system that documents the severity and enables triage of the most severe problems. Depending on the nature of the issue, technical problems may be dealt with directly by Connie staff or in certain situations may be raised to the attention of the applicable Connie vendor. For all reported and verified problems, Connie will work to find a resolution in a timely manner and update Participants of actions taken as appropriate. The help desk provides support 24 hours a day, seven days a week, including weekends and holidays.

10. Audit

All Participants are required to monitor, and audit access to and use of, their information technology systems in connection with Connie Services and in accordance with their usual practices based on accepted health care industry standards and Applicable Law. In the event Connie wishes to exercise its right to audit the Participant, Participant will provide Connie with monitoring and access records upon request. Connie regularly reviews the usage of Participating User access of patient records and will enforce any misuse of a Participating User to include and up to termination of Connie Services access. Notwithstanding, Connie does not, and does not endeavor to, review each access by each Participant User. Connie uses a privacy tool for additional monitoring of all user activities around protected health information access to ensure all provisioned accounts are being used appropriately and to protect protected health information; however, it is ultimately the Participant's obligation to ensure the appropriate use of Connie Services by Participant and Participant Users.

11. Report of Breach

In the event that a Participant discovers that data has been inappropriately sent, received, found, or used through Connie Services by the Participant or a Participant User, the Participant must notify Connie of the event within ten (10) business days of discovery or as otherwise required by the Agreements. As soon as reasonably practicable, but in no event later than thirty (30) calendar days of discovery, Participant will provide Connie with the identification of each individual whose protected health information has been or is reasonably believed to have been breached during such incident. The Participant will cooperate with Connie as to further investigation or responsive action reasonably requested or taken by Connie to respond to the event. The notification shall be treated by Connie as Confidential Information, except as otherwise required pursuant to Applicable Law or as used or disclosed by Connie in connection with exercise of Connie's rights and/or obligations under the Agreements to defend its actions in any process or proceeding begun by or involving the Participant or Applicable Law.

In the event of a Breach of protected health information sent, received, found, or used via Connie Services requiring notification to individuals under Applicable Law, the parties will handle the notification as set forth in the Agreements.

12. Connie Board of Directors and Management Advisory Groups

12.1 Connie Board of Directors

Connie is governed by a Board of Directors, the composition of which is set forth by Conn. Gen. Stats. Sec. 17b-59g and includes the following members:

- One member who has expertise as an advocate for consumers of health care, appointed by the Governor;
- One member who has expertise as a clinical medical doctor, appointed by the president pro tempore of the Senate;
- One member who has expertise in the area of hospital administration, appointed by the speaker of the House of Representatives;
- One member who has expertise in the area of corporate law or finance, appointed by the minority leader of the Senate;
- One member who shall have expertise in group health insurance coverage, appointed by the minority leader of the House of Representatives;
- The Chief Information Officer and the Secretary of the Office of Policy and Management, or their designees, who shall serve as ex-officio, voting members of the Board of Directors;
- The health information technology officer, designated in accordance with section Conn. Gen. Stats. Sect. 19a-754a, who shall serve as chairperson of the Board of Directors; and
- The Commissioner of Social Services, or the commissioner's designee, who shall serve as an ex-officio, voting member of the Board of Directors.

The Connie Board of Directors meets regularly to review Connie's financial performance, director reports, recommendations from advisory groups, and other topics as needed to progress the mission of Connie. Current board members can be found listed on Connie's website.

The Connie Board of Directors also has two sub-committees, the Finance & Audit Committee and the Privacy, Security, & Confidentiality Committee. The general responsibilities of each committee are defined in their respective charters. Decisions made by the Connie Board of Directors will be final as to Connie, to the extent permitted by law.

12.2 Connie Management Advisory Groups

Connie has developed a model that includes an Operations Advisory Committee and a Clinical Advisory Council, collectively "the Advisory Groups", to provide guidance and input to Connie management on certain key decisions during the development and operations of Connie Services. The Advisory Groups are intended to be broad-based to ensure that a breadth of interested organizations have the opportunity to participate and represent their constituencies.

The Operations Advisory Committee is made up of representatives from Participants who have signed the QDSOA. The Clinical Advisory Council is made up of clinical and subject matter experts appointed by Connie management.

13. Provider Authorization

Participant Users, by electing to receive data through Connie Services, authorize Connie to transmit results, reports, and other patient information directly from Participant Users' providers, such as clinical laboratories and radiology centers. Participant Users further acknowledge the following:

1. All ancillary providers represent that, at the time the data is transmitted by the ancillary provider, the data transmitted is an accurate representation of the data that is contained in, or available through, the ancillary provider's system;
2. Nothing in the Agreements, this Operating Policies and Procedures document, or otherwise will impose responsibility or liability on ancillary providers related to the accuracy, content, or completeness of any data or information provided in connection with a message or otherwise;
3. As a data source, ancillary providers do not assume any control over or responsibility for the clinical decision making as to any patient of a Participant; and
4. If not approved by ancillary provider for delivery of a report of record, access to such data through the Connie Services is neither designed nor intended to replace ancillary provider's principal method of results delivery to Participant and does not constitute a "Report of Record." The official list of ancillary providers participating in Connie can be found on the Connie website at https://conniect.org/for-organizations/.

14. Standards

Connie aims to support Connie Services in a standards-compliant manner and will use industry standard practices and generally accepted standards when possible and appropriate that are recognized by State, Federal, or industry authorities. Connie maintains a Use Case Implementation Guide provided to Participants that details the interface standards and content specifications that Connie supports.

15. Information Blocking Rule

The 21st Century Cures (CURES) Act and its implementing regulation (the Information Blocking Rule (IBR)) prohibits “information blocking,” which is a practice engaged in by an actor that interferes with the access, use or exchange of Electronic Health Information. The IBR requires actors, like Health Information Networks, to fulfill requests for Electronic Health Information (EHI). This requirement is entirely consistent with Connie’s goals. The IBR also expressly recognizes that actors, like Health Information Networks, must impose restrictions on those who seek to access, exchange, or use EHI because those restrictions promote a larger public purpose such as making certain that the privacy and security of EHI is protected and that only those who are authorized can access, exchange, or use EHI. The IBR includes several specific Exceptions which an actor can use to decline to fulfill a request for EHI in certain situations. The IBR’s content and manner exception specifically allows an actor and a data requestor to mutually agree on the terms under which the requestor will access, exchange, or use EHI.

The Agreements and these Operating Policies and Procedures are designed to comply with the content and manner exception by specifying the mutually agreed upon terms and conditions that govern the access, exchange, and use of information by Participants. Other IBR exceptions may also apply from time to time depending upon the facts and circumstances that are present when a request for EHI is presented to Connie. Connie will document its reasons for not fulfilling a request for EHI so that a record exists in the event that an information blocking complaint is filed. Connie will also review and update its Agreements and the Operating Policies and Procedures from time to time in an effort to ensure that they remain consistent with the IBR and any other applicable law.

16. External HIE Participation

16.1 Current Participation

From time-to-time, Connie will participate with External HIEs as defined by the Connie Agreements. These External HIEs include, but may not be limited to, National Networks or other state or local HIEs. At this time, Connie shares information with External HIEs only for the purpose of treatment. Any additional purpose for sharing would be approved by the appropriate Connie Advisory Committee in accordance with the Connie Agreements and these Operating Policies and Procedures.

16.2 New Participation Procedures

In collaboration with the Connie Councils, Connie may determine it is beneficial to Connie and Connie Participants to participate with additional External HIEs. Connie Councils and/or Board sub-committees will assist Connie to perform privacy and security reviews of the External HIEs. Additionally, Connie will ensure that any External HIE agreements are substantially similar to the Agreements and the Connie Operating Policies and Procedures relative to privacy and security, data storage and transmission, insurance, liability provisions, and permitted purposes for data disclosure and redisclosure.