Privacy

- Since its inception, Connie has and continues to comply with all federal and state laws and regulations on data sharing and privacy.
- We have adopted a comprehensive data privacy protection program to ensure that all health information is used and disclosed only as permitted or required by law.
- As Attorney Gold pointed out, the basis for this program is found in Connie's implementing statutes which require Connie to keep confidential information secure and to meet all state and federal privacy requirements.
- These requirements are reinforced and expanded upon in Connie's contract with the state which requires Connie to safeguard all personal information and ensure that the use and disclosure of such information complies with all applicable law.
- Connie then extends those same safeguards and requirements in its participation and business associate agreements with its participating organizations all of which require Connie to disclose health information only as permitted or required by law.
- Further, Connie's Board codified these requirements and safeguards in a Data Release Policy (available on our website) that details the circumstances in which Connie may disclose health information.
- Connie maintains an active Board-level Privacy, Confidentiality, and Security Committee with public meetings whose responsibility it is to ensure that Connie is living up to its expectations with respect to its legislative mandate, its contractual obligations, and the law. The Privacy, Confidentiality, and Security Committee is made up of Connecticut stakeholders including patient advocates, health systems, and behavioral health organizations.

Patient Consent and Opt-Out

- Connie is a voluntary benefit for the citizens of Connecticut. Patients have the right and the ability to opt out of data sharing with Connie with a simple form available on our website (https://www.conniect.org/optout). Patients only need to opt out once for all providers; once they opt out, their health data is deleted from Connie, and patients can opt back in at any time.
- Connie's Board adopted an opt-out consent model based on a report from the HITAC Consent Workgroup and public comments to OHS following their request for feedback to the HIE Consumer Consent Policy. This is consistent with HIPAA and most other healthcare organizations in the state. Data is sharable for HIPAA-compliant purposes unless a patient specifically opts out.

- Connie's consent policy does require affirmative consent to share certain sensitive information including SUD data from Part 2 organizations.
- Connie does require all participating organizations to review applicable state and federal laws regarding data sharing and privacy to determine what their obligations are.

Patient Empowerment

- In addition to secure data exchange, our enabling legislation laid out a mandate for Connie to empower patients. Our commitment to that aim includes the development of a patient portal where patients will be able to see and manage their health information as well as provide a mechanism for them to manage their affirmative consent decisions.
- We have convened a Patient and Family Advisory Council made up of patient stakeholders to provide input and feedback as we continue to develop our portal and its functionality.

Cybersecurity

- Ensuring that health data is private and secure is a top priority and a promise to Connecticut patients for Connie. Connie has robust privacy and security controls and protocols, including thorough incident response and disaster recovery plans for cyberattacks.
- Our IT infrastructure has received the most stringent third-party security certifications – including HITRUST and EHNAC. These certifications require ongoing updates, training, and recertification. Additionally, our IT infrastructure partner participates in voluntary tabletop incident exercises with other security industry leaders and conducts annual security audits including SOC-2 Type 2 testing, cybersecurity testing, HIPAA/HITECH and annual penetration testing by independent cybersecurity firms.
- This is all overseen by the Privacy, Security, and Confidentiality Committee of the board.
- We strongly support proposals to have Connie be responsible for investigating, responding to, and mitigating any data breach occurring at Connie or a Connie vendor or subcontractor. Connie encourages OHS to adopt regulations that both include this requirement and state definitively that health care providers are not, and shall not be, responsible for investigating, responding to, or mitigating any such Connie breach. We believe that this requirement is vital to ensure patient transparency and to reduce patient confusion. Connie wants to avoid providers incurring breach response obligations due to a Connie breach and patients receiving multiple or no notices of a Connie breach. Connie believes that having the State-Wide Health Information Exchange be responsible for all of these matters,

with direct oversight by OHS, is the most practical method to avoid such harms to patients and providers.

Connie Resources:

- Connie Website: www.conniect.org
- Connie's Data Release Policy: https://www.conniect.org/_files/ugd/e7f8c9_2bf7f2d145de454a94bea7cd3bf3652d.pdf
- Patient Opt-Out: https://www.conniect.org/optout
- Onboarding Materials including Provider Communications Toolkit: https://www.conniect.org/onboardinginformation