Privacy Policy

1.0 Purpose

1.1 The Atrium Health CareConnect policy on patient/consumer privacy considers patients'/consumers' rights and expectations while balancing the need for health care providers to have information that enables them to make informed decisions and ultimately provide better quality health care services.

1.2 In order to maintain an appropriate level of security and to protect patient/consumer data from unauthorized access and disclosure, this policy defines the access controls and parameters necessary to achieve this protection and to promote reliable operation of the health information exchange (HIE).

2.0 Definitions

2.1 "Health Information" means any information, in electronic or physical form, regarding patient/consumer medical history, mental or physical condition, or treatment.

2.2 "Individually Identifiable" means that the information includes an element or elements relating to an individual such that, when taken alone or in combination with other publicly available information, it becomes sufficient to allow identification of the individual.

2.3 "Health Care Provider" means a health professional licensed in North Carolina and/or South Carolina with the authority to order or prescribe clinical tests and diagnostics, including physicians as defined by Title 18, Section 1861(r) of the Social Security Act, and clinical medical professionals who are licensed to diagnose and treat patients/consumers under the supervision of such licensed professionals.

2.4 "Member Organization" means the health care facility or entity that has contracted with Atrium Health CareConnect for access to and participation in the Atrium Health CareConnect HIE.

2.5 "Data Sending Organizations" means those Member Organizations that make Health Information (e.g. lab results) available to Health Care Providers through the Atrium Health CareConnect HIE.

2.6 "Users" means those individuals who are under the employ or control of a Member Organization, are designated by the Member Organization for access to the Atrium Health CareConnect HIE, and enroll in the Atrium Health CareConnect HIE to receive clinical results and reports. Atrium Health CareConnect HIE Users are Health Care Providers and their designated staff as permitted by Atrium Health CareConnect policy, who must agree to maintain the privacy and security of the information that they obtain from the Atrium Health CareConnect HIE. Atrium Health CareConnect HIE Users receive clinical results and reports and, when available, may also Query the Atrium Health CareConnect HIE for clinical history.

2.7 "User Roles" means the rules defined by Atrium Health CareConnect and assigned to Users, which establish the parameters on a User's level of access to Individually Identifiable Health Information through the Atrium Health CareConnect HIE.

2.8 "Query" means a system search for Health Information about a patient/consumer by an authorized User who has an established treatment relationship with that patient/consumer, conducted via the Atrium Health CareConnect HIE on a Need-to-Know basis.

2.9 "Need-to-Know" means the standard or threshold of justification required by law and by Atrium Health CareConnect policy of a User in order for that User to view patient/consumer information in the Atrium Health CareConnect HIE. In order to safeguard patient/consumer privacy, the Atrium Health CareConnect HIE Users are authorized to receive access only to the minimum functions and privileges required for performing their jobs.

3.0 Policy

3.1 This policy is applicable to all Users and Member Organizations of the Atrium Health CareConnect HIE. All Users of the Atrium Health CareConnect HIE, both senders and receivers of data, have signed the appropriate legal agreements to support the privacy and security of data in the Atrium Health CareConnect HIE, in compliance with state and federal law and the Atrium Health CareConnect Terms of Use.

3.2 This policy does not supersede or replace any Health Insurance Portability and Accountability Act (HIPAA) requirements or state-required privacy and security policies in use by individual Atrium Health CareConnect HIE Users and Member Organizations. All Users and Member Organizations must abide by the requirements under HIPAA; nothing in this policy and any related policies and agreements shall assign Users' and Member Organizations' direct responsibility to comply with HIPAA to the Atrium Health CareConnect HIE.

3.3 Patient/consumer privacy is of material importance. Atrium Health CareConnect requires Users and Member Organizations to comply with all applicable federal laws and regulations dealing with privacy, security and breach notification, including 45 CFR Part 160 and 164.

3.4 Health Care Providers and/or Users of the CareConnect HIE should not print records from the HIE to provide a patient access to their medical record. The individual EMR system or Health Information Management department of the Data Sending Organizations (not HIE) should be the only the source of medical records provided to patients upon request or otherwise.

4.0 Restrictions on the Use and Disclosure of Individually Identifiable Health Information

4.1 **Disclosure of Individually Identifiable Health Information**. Patient/consumer information in the Atrium Health CareConnect HIE shall not be sold or disclosed to any third party for any commercial or unauthorized activity.

4.2 **Query Access**. Only Users enrolled in the Atrium Health CareConnect HIE who have an established treatment relationship with a patient/consumer are permitted access to that patient/consumer's information available through the Atrium Health CareConnect HIE. Users who are emergency care personnel are permitted access to the Atrium Health CareConnect HIE whereby they can access patient/consumer records in emergency care situations on a Need-to-Know basis.

4.3 **Special Restrictions.** Users shall not use the Atrium Health CareConnect HIE for any purposes that would be in violation of their or their Member Organization's own privacy policies, or that could lead to, or appear as, anti-trust violations, breaches of confidentiality (including of third-party contracts), competitive purposes, to sell information, or infringement of any proprietary or intellectual property rights.

4.4 **Compliance with Law**. Users who violate patient/consumer privacy are subject to consequences, up to and including immediate termination of access to the Atrium Health CareConnect HIE and legal action.

5.0 Patient/Consumer Notification

5.1 Data Sending Organizations shall implement appropriate procedures to inform, and provide sufficient evidence upon request that they have informed, their patients/consumers (1) that they use the Atrium Health CareConnect HIE to exchange their patients'/consumers' information with other Atrium Health CareConnect HIE Users, and (2) of their patients'/consumers' right to opt-out from having Individually Identifiable Health Information about them made available for Query by authorized Users of the Atrium Health CareConnect HIE. Prior to providing patient/consumer information to the Atrium Health CareConnect HIE, Data Sending Organizations are responsible for verifying the information and compliance with all necessary requirements.

5.2 Atrium Health CareConnect may make sample resources available to Data Sending Organizations to respond to patient/consumer inquiries about the Atrium Health CareConnect HIE (e.g., brochures, answers to frequently asked questions, talking points, and forms for opting-out). Such resources are provided as a courtesy and are utilized at the Data Sending Organization's own risk.

6.0 Patient/Consumer Opt-Out

6.1 Patients/consumers may decide not to participate in the Atrium Health CareConnect HIE, or "opt-out", by submitting an Opt-Out Request Form to the designated Data Sending Organization.

6.2 If a patient/consumer opts-out, the designated Data Sending Organization must immediately notify Atrium Health CareConnect by sending the Request for Opt-Out Form, and that patient's/consumer's Individually Identifiable Health Information will not be available to Users (including emergency care personnel) upon a Query of patient/consumer information in the Atrium Health CareConnect HIE. Opt-outs can take up to two business days (Monday through Friday, excluding holidays) from Atrium Health CareConnect's receipt of the notification to become effective.

6.3 Patients/consumers who have opted out may choose to participate in the Atrium Health CareConnect HIE again at any time by submitting a Cancellation of Opt-Out Request Form to the designated Data Sending Organization.

6.4 If a patient/consumer cancels a previous opt-out request, the designated Data Sending Organization must immediately notify Atrium Health CareConnect by sending the Cancellation of Opt-Out Request Form, and Atrium Health CareConnect will, in a timely manner and according to the procedures that are established, include that patient's/consumer's Individually Identifiable Health Information in the Atrium Health CareConnect HIE as directed by the designated Data Sending Organization.

7.0 Amendment of Data

7.1 Once patient/consumer data has been provided to the Atrium Health CareConnect HIE, any change to that data based upon patient/consumer request to amend such data can only be made by the Data Sending Organization that originally contributed the data to the Atrium Health CareConnect HIE. Atrium Health CareConnect does not have the authority or access to amend such data.

7.2 Amendment requests that are received by Atrium Health CareConnect will be forwarded to the relevant Member Organization for review and determination. Member Organization is responsible for complying with the requirements under 45 CFR 164.526, including timeliness and documentation of response to the patient.

8.0 Breach Notification

8.1 Users and Member Organizations are responsible for safeguarding against any breaches of privacy or security, including those that could cause harm to the patient/consumer.

8.2 If a User or Member Organization (or a business associate of the User or Member Organization under HIPAA) discovers that a privacy breach as defined by HIPAA, or a security breach as defined by state law, of patient/consumer information has occurred, the breach must be reported immediately to the Atrium Health CareConnect designated privacy official.

8.3 The User and Member Organization must cooperate with the Atrium Health CareConnect designated privacy official, and shall make reasonable and timely efforts to mitigate the effects of the breach and implement any necessary safeguards. Users and Member Organizations will be responsible for any breaches caused by their contractors or agents, including business associates.

8.4 Unless expressly agreed otherwise by the parties, the Member Organization will be responsible for determination of whether a breach has occurred with its information and for making the proper notifications.

8.5 Atrium Health CareConnect will follow its monitoring and breach notification procedures policy.

9.0 Access Controls

9.1 Access rights and parameters, which are the system-level security settings that grant or deny authorization to view Individually Identifiable Health Information in the Atrium Health CareConnect HIE, are granted to Atrium Health CareConnect HIE Users based on the following factors:

9.1.1 **User Authentication**. Any User accessing the Atrium Health CareConnect HIE must be authenticated by the system's verification process to properly identify and/or credential the User to gain authorized access to the Atrium Health CareConnect HIE application. The level of authentication will correspond appropriately to the designated access rights.

9.1.1.1 To obtain access to Atrium Health CareConnect HIE, an authorized User must enter his/her unique User identification and supply an individual User password.

9.1.1.2 To obtain a new password for the Atrium Health CareConnect HIE, Users must be able to provide the answers to unique questions selected and answered by the User at the time of set-up.

9.1.1.3 All Users will be required and prompted to change their passwords periodically as required by Atrium Health CareConnect and consistent with HIPAA.

9.1.1.4 Passwords must be promptly changed upon suspicion of any disclosure to unauthorized parties.

9.1.1.5 At the time a User is no longer associated with or employed by a Member Organization, the Member Organization is required to notify Atrium Health CareConnect so that the User may be terminated in Atrium Health CareConnect.

9.1.1.6 Atrium Health CareConnect may periodically ask Member Organization to validate its User list. If the Member Organization does not respond within the designated response time, the access rights of unauthenticated Users may be suspended without further notice.

9.1.2 **User Roles and Job Responsibilities**. The Member Organization is responsible for accurately designating which roles the User should have for the Atrium Health CareConnect HIE through the Member Organization. Users should be granted access to information on a Need-to-Know basis; that is, Users should only receive access to the minimum functions and privileges required for performing their jobs. Member Organizations are responsible for verifying that their Users are authorized to have access based on their then current function at the Member Organization.

9.1.3 **Unique User identification**. Each User is assigned a unique identifier that supports individual accountability and enables tracking.

9.1.3.1 The User is responsible for all actions conducted under his/her log-in credentials.

9.1.3.2 Under no circumstances should a User's log-in credentials be shared.

9.1.3.3 If a password is suspected of being disclosed to an unauthorized party, it must be promptly changed. Atrium Health CareConnect reserves the right to terminate the Atrium Health CareConnect HIE access of a User whose password has been disclosed.

9.1.3.4 Atrium Health CareConnect will routinely monitor User accounts for activity and may disable those that have been inactive for 90 or more days.

10.0 Audit Controls

10.1 Atrium Health CareConnect shall monitor access to Individually Identifiable Health Information on a regular and scheduled basis to verify appropriate use of the Atrium Health CareConnect HIE. This will include logging and monitoring of system activity, including: User log-in identification; User name; User's Member Organization; date and time; patient/consumer account that was accessed.

10.2 Member Organizations and Users will fully comply with any inquiries or investigations into access by a User and promptly cooperate with Atrium Health CareConnect to validate use.

10.3 Access to the Atrium Health CareConnect HIE for Users determined to be a risk to security will be suspended, terminated and/or flagged for enhanced security review commensurate with the potential risk.

10.4 As part of the Atrium Health CareConnect HIE User security audit, Atrium Health CareConnect may identify Users that have potentially "misused" the Atrium Health CareConnect HIE by accessing Individually Identifiable Health Information without meeting the Need-to-Know standard.

10.5 Upon a determination that a User has not complied with this Privacy Policy, the User's access authority may be suspended, limited or revoked. If a Member Organization has a pattern of inappropriate Users, Atrium Health CareConnect may terminate that Member Organization's rights to the Atrium Health CareConnect HIE and hold them in breach of any relevant agreements.

11.0 User Liabilities

11.1 Users and Member Organizations responsible for a breach of this Privacy Policy, including inappropriate review or viewing of patient/consumer information without a Need-to-Know for diagnosis, treatment, or other lawful use, may be subject to the following:

11.1.1 Action by Atrium Health CareConnect, including suspension or termination of access to the Atrium Health CareConnect HIE;

11.1.2 Fines and penalties assessed by federal, state or local agencies;

11.1.3 Reporting to federal, state or local agencies;

11.1.4 Being held liable for any damages to Atrium Health CareConnect; and/or

11.1.5 Action by the patient/consumer.