DOCUMENT 26:
HEALTH INFORMATION EXCHANGE POLICIES AND PROCEDURES

HEALTH INFORMATION EXCHANGE

Policies and Procedures

I. Vision, Mission, Goals and Structure

A. Vision. The Exchange's vision is to develop and maintain an electronic health information system that provides a longitudinal electronic medical record for _____ _____ patients that can be accessed and updated in real time by authorized health care providers.

B. Mission. The Exchange's mission is to enhance patient safety and the efficient provision of quality patient care in _____ _____.

C. Goals. The Exchange will enhance patient care by:

1. Speeding health care providers' access to critical patient information.

2. Providing a longitudinal view of the patient's medical history across Exchange health care providers.

3. Reducing health care costs through automation and reducing duplicative tests.

4. Reducing medical errors created by incomplete or incorrect information in patient medical records.

D. Governing Body. The governing body of Exchange is the Board of Directors of the _____ ("Network").

II. Authorized Users

A. User Enrollment

1. Network member hospitals may enroll:

   a. Exchange physicians who have staff privileges at a Exchange hospital;
   b. Those physician's office staff;
   c. Exchange hospital-employed RNs who are primarily assigned to the Emergency Department ("ED") and Exchange hospital ED physicians;
   d. Exchange health care providers such as nursing home and health department staff; and
   e. Exchange hospital-employed licensed clinicians who are performing a dedicated case management role.

   (collectively referred to as "Authorized Users") to access electronic patient data through Exchange. The term "physician" as used in this section shall

include Doctor of Medicine (MD), Physician Assistant (PA), Nurse Practitioner (NP), Doctor of Osteopathic Medicine (DOM), Doctor of Podiatric Medicine (DPM), Doctor of Dental Surgery (DDS)**,** Doctor of Psychology (PsyD), Certified Nurse Midwife (CNM), residents and Certified Registered Nurse Anesthetist (CRNA).

2. Each Network member hospital will be responsible for initiating, updating, monitoring, controlling, and removing or suspending access of its Authorized Users in Exchange.

3. Once the enrolling hospital provides an Authorized User with training to familiarize them with Exchange, the enrolling hospital will assign him or her a: i) User ID that contains the abbreviation of the hospital (see below), the user's first initial, and the user's last name (*e.g.*, RHJJones); and ii) password that contains at least 7 digits including at least 2 alpha digits and 2 numeric digits. Authorized Users must change their passwords at least every 180 days and may not re-use a password. Passwords shall be case sensitive.

_____: ___	_____: ___
_____: ___	_____: ___
_____: ___	_____: ___
_____: ___	_____: ___
_____: ___	_____: ___
_____: ___	_____: ___
_____: ___	_____: ___
_____: ___	Network_____: net

4. The first time an Authorized User logs into Exchange, he/she will view an Exchange Agreement detailing the permitted uses of the system, HIPAA compliance requirements and the user's roles and responsibilities. The Authorized User must click "I Agree" to continue using Exchange. Each Authorized User's consent to the agreement will be logged in the audit trail. The Authorized User may print a copy of the Agreement from their "preferences" section in Exchange.

5. The enrolling hospital immediately shall remove an Authorized User's access to the Exchange if the user is no longer employed or otherwise associated with the hospital.

6. Exchange automatically shall remove an Authorized User's access to the system if the user has not accessed the system during a one-year period.

B. User Restrictions

1. Authorized Users shall use the Exchange solely to access patient information in the following situations:

   a. Pursuant to the purposes specified in 45 C.F.R. §164.506(c) (the HIPAA regulations):

- For treatment activities of any health care provider.
- If the patient information was created at the covered entity for which the Authorized User works, for the payment or health care operations purposes of that covered entity.
- If the patient information was not created at the covered entity for which the Authorized User works, for the payment activities of that covered entity, and for the health care operations activities of that covered entity, if that entity either has or had a relationship with the patient and the information is needed to conduct quality assessment and improvement activities or review the competence or qualifications of healthcare professionals.

b. Pursuant to a valid authorization when required by 45 C.F.R. §164.508 or 42 C.F.R. § 2.1, *et seq.*, or pursuant to a valid authorization or consent when required by North Carolina law.

2. Each enrolling hospital must place appropriate restrictions on each Authorized User upon enrollment, as follows:

a. **Exchange Physicians.** Physicians with staff privileges at a Exchange hospital may have access to any patient's information when they are identified as the patient's primary, admitting, attending, consulting, or operating physician at any Network member hospital. If a Exchange physician wants access to other patients' information, a message will appear stating: "Our records indicate that you do not have an existing relationship with the patient you have selected. To continue, you agree that you need this information for the continuing care and treatment of the patient. Your access to this information is subject to audit and review." To access that patient's information, the Exchange physician must click on the "Continue" button and the override will be recorded in the audit trail.

b. **Exchange Physician Office Staff.** These individuals may have access to any patient's information only when a physician associated with that office is identified as the patient's primary, admitting, attending, consulting, or operating physician at any Network member hospital. These individuals have no override privileges to view other patients' information. However, a Network member hospital may allow at least one key member of each physician's office staff to have override privileges to view other patients' information, subject to the same audit and review process as the physicians' override privileges.

c. **Exchange ED Physicians and ED Clinicians**. These individuals may have access to all patient information and may access any patient information when such information is needed for the patient's continuing care and treatment, subject to the same audit and review process. Each Exchange hospital's ED clinical director or hospital clinical director shall determine which ED RNs shall have access privileges.

d. **Exchange Health Care Providers**. These individuals may have access only to patient information at the Exchange hospital that enrolled the user and cannot access patient information from other Exchange hospitals. These users may only view a

patient's information if the enrolling hospital has created a link between the user and the patient to establish a relationship. These individuals have no override privileges to view other patients' information. These users may not search for patients at other Exchange hospitals.

e. **Exchange Hospital Case Managers**. These individuals may have access to any patient's information when the user is serving as a case manager for the patient and the information is needed for the continuing care and treatment of the patient. The Exchange hospital desiring to provide access to the user must establish a link between the user and a patient. These individuals have no override privileges to view other patients' information.

3. Exchange will:

   a. Log-out an Authorized User following ten minutes of inactivity in the system.
   b. Lock out an Authorized User following three failed log-in attempts. When this occurs, a message will appear directing the user to contact the enrolling hospital.

4. Exchange will establish warnings and automatic e-mail alerts to the Data Provider and to Network when it detects erratic usage or anomalies by an Authorized User or any other user (*e.g.*, an Authorized User overrides the system five times within five minutes).

C. Audit Trails

1. Exchange will record each time an Authorized User accesses the Exchange and will record every item of patient information accessed by the Authorized User.

2. The audit trail will identify whether the Authorized User "overrode" the system to access information of patients with whom the user does not have a pre-existing relationship. Since ED clinicians and ED physicians are not required to have a pre-existing relationship with a patient, their overrides are not recorded in the audit trail.

3. Each Network member hospital routinely will review the audit trails of information accessed from its facility to identify and investigate any potential abuses or violations of the Exchange Policies and Procedures or applicable federal or state laws or regulations.

4. Upon request, each Network member hospital will follow its internal policies and procedures for providing an accounting of disclosures to the patient or patient's representative requesting the accounting, in order to indicate who has accessed the patient's information for treatment provided at that member hospital's system.

D. Sanctions of Users

1. Each Network member hospital will follow its internal policies and procedures to sanction its Authorized Users who inappropriately access patient information from the Exchange.

2. If a Network member hospital, following an investigation of an alleged violation, concludes that one of its Authorized Users has inappropriately accessed information of a patient treated at that hospital, the hospital will follow its internal policies and procedures to sanction the user.

3. If a Network member hospital, following an investigation of an alleged violation, concludes that a user authorized by another hospital has inappropriately accessed information of a patient treated at the first hospital, the first hospital will contact the authorizing hospital and request that the authorizing hospital follow its internal policies and procedures to investigate the apparent violation and, if appropriate, sanction the user. The authorizing hospital thereafter shall notify the first hospital in writing that it has concluded its investigation, determined that a violation did or did not occur, and taken appropriate action without specifying the particular action taken. If the first hospital concludes that the same user has inappropriately accessed patient information a second time, that hospital will request that the authorizing hospital revoke the user's privileges to use Exchange. Any disputes between hospitals about sanctions of users will be resolved by the Exchange Task Force, whose conclusion shall be final.

4. If a Exchange member hospital determines that a breach has occurred, the hospital will notify Network. Network will then notify other hospitals of the breach and suggest that they conduct an audit to determine if the breaching party inappropriately accessed their data.

III. Availability of Patient Information

A. Hospital Privacy Notices.

1. Each Network member hospital will include a clause in its Notice of Privacy Practices indicating that patient data may be provided to third parties in various formats. The clause shall be substantially as follows:

> "In order to efficiently coordinate the treatment, payment, and health care operations aspects of your care, we may disclose your PHI in any format that we determine is secure and expeditious, *e.g.*, verbally, electronically, via fax, and/or in paper form."
>
> "Para coordinar eficientemente el tratamiento, el pago, y los aspectos de la operación del cuidado de la salud, es posible que publiquemos su PHI en cualquier formato que determinamos es seguro y conveniente, por ejemplo, verbalmente, electronicamente, por medio de fax, y/o en palabra escrita."

B. Restrictions on Patient Information

1. Each Network member hospital will allow its patients the right to prohibit the access of all their data or data from a particular encounter(s) through Exchange. Exchange will provide an option that allows hospitals to block access to a patient's data through Exchange. If a patient has chosen this option, when a query is made about that particular

patient or about electronic information to which that patient has prohibited access, Exchange will indicate "NOTE: This patient's medical record has been excluded from view in Exchange. Please contact the applicable hospital or the patient for additional details". If a patient desires to revoke or change his or her opt-out decision, the patient must contact the hospital that initially opted out the patient to make any revisions. Only the hospital that initially opted out the patient has the ability to make these revisions.

2. Exchange will not allow any Authorized User access to any patient information from a dedicated acute in-patient or outpatient psychiatric unit or an in-patient or outpatient substance abuse facility, as designated by each Network member hospital. Each hospital shall have the right to exclude from Exchange non-hospital patient data that is contained within its clinical information system.

3. Exchange will allow Authorized Users to access patient information from all lab results and medication histories to provide complete information for the continuing care and treatment of the patient.

4. Exchange will allow Authorized Users to access patient information dating as far back as the information is maintained on each Network member hospital's information system. Each Network member hospital shall maintain patient information on its information system for at least two years following a patient's discharge. If a Network member hospital archives certain patient data, Exchange shall access the archived data in the order specified by the hospital.

5. Exchange will allow Authorized Users to access draft reports of patient information that are not yet approved and signed by a physician. The status of these reports will be designated the same in Exchange as each Network member hospital's legacy system designates the status. It is recognized that physicians in some member hospitals cannot electronically sign the drafts, and accordingly those reports will always be designated as something other than "final" or "signed".

6. Network member hospitals shall notify the Exchange and Access Provider and/or Host in advance of any planned changes in their legacy system, firewalls or VPN that may impact the data accessed by Exchange or the connectivity to Exchange.

C. Response to Patient Requests

1. When responding to requests for release of patient information, Network member hospitals shall not release data accessed or obtained through Exchange. Each hospital shall only disclose data from its patient medical records. The information provided by Exchange does not constitute the patient's medical record and the system does not maintain patient data. Exchange simply queries and collates patient data from the participating providers.

2. Each Network member hospital will follow its internal policies and procedures for responding to patients' or patient representatives' requests for a) access to patient information, b) amendments to the patient's information, and c) restrictions on the access, use, or disclosure of patient information.

3. If a Network member hospital receives a request to access or to amend patient information regarding treatment that was provided by another facility, the hospital will forward that request to the treating facility and the treating facility shall be responsible for responding to the request for access or amendment.

4. If a Network member hospital receives a request to restrict the access, use, or disclosure of patient information regarding treatment that was provided by another facility, the hospital will forward that request to the treating facility and the treating facility shall be responsible for responding to the request for restrictions.