GUIDELINES AND PROCEDURES FOR

COMPLIANCE WITH EHEALTH EXCHANGE REQUIREMENTS

POLICY #2018-01

Background:

UConn Health participates in the eHealth Exchange (the "Exchange"), an electronic health information exchange among federal governmental agencies and non-federal organizations. In order to participate in the Exchange, UConn Health entered into a contract (called the Data Use and Reciprocal Support Agreement, or "DURSA") agreeing to comply with specific requirements for using the Exchange. The DURSA requires UConn Health to have written policies, procedures and guidelines for compliance with these requirements.

UConn Health's existing policies and procedures address all but the following two requirements:

(1) The DURSA breach notification requirements (which are narrower than the breach notification requirements under HIPAA and apply in only very limited circumstances); and

(2) The DURSA requirements for limiting certain uses and disclosures of information transmitted via the Exchange (which are substantially similar to HIPAA's requirements around uses and disclosures for treatment, payment, or health care operations, but with some subtle differences that warrant additional guidelines).

These Guidelines for Compliance with eHealth Exchange Requirements ("Guidelines") are intended to facilitate UConn Health's compliance with these two requirements.

I. BREACH NOTIFICATION

A. Definitions:

The DURSA breach notification requirements apply only to a very limited type of breach, referred to in these Guidelines as a "DURSA Breach."

A "DURSA Breach" is:

- Any unauthorized acquisition, access, disclosure, or use of information contained within an electronic transmission on the Exchange (such information is referred to as "message content") ***while transacting such message content pursuant to the DURSA.***

If a breach (or suspected breach) occurs *at the same time* that UConn Health is sending, requesting, receiving, or accessing message content through the Exchange, it is a DURSA Breach (or suspected DURSA Breach, as applicable).

DURSA Breaches do not include breaches that are not directly related to transacting message content on the Exchange. DURSA Breaches also do not include any unintentional acquisition, access, disclosure or use of Exchange message content by a UConn Health employee (or other individual acting under the authority of UConn Health), if:

- The acquisition, access, disclosure or use was made in good faith and within the scope of the employee's/individual's duties, and

- The message content is not further acquired, accessed, disclosed, or used by the employee/individual.

B. Guidelines:

1. Suspected DURSA Breach: Within one (1) hour of discovering information that leads UConn Health to reasonably believe that a DURSA Breach may have occurred, the UConn Health Security Officer will provide notice of the suspected DURSA Breach to the Exchange Coordinating Committee and any Exchange participants whose information may have been breached. (The Coordinating Committee is a group of individuals authorized under the DURSA to oversee, facilitate and support Exchange participants.)

2. Actual DURSA Breach: As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a DURSA Breach has occurred, the UConn Health Security Officer will provide notice of the DURSA Breach to the Exchange Coordinating Committee and other Exchange participants likely impacted by the breach.

3. In all cases, notification to the Exchange Coordinating Committee should be provided via email (admin@sequoiaproject.org) or by telephone ((571) 327-3640) and should include sufficient information for the Coordinating Committee to understand the nature of the actual or suspected DURSA Breach.

4. UConn Health will reasonably cooperate with other Exchange participants and Coordinating Committee in the investigation of actual and suspected DURSA Breaches.

II. LIMITING CERTAIN USES AND DISCLOSURES

A. Introduction

HIPAA broadly permits UConn Health to use and disclose protected health information ("PHI") without an authorization for treatment, payment and health care operations purposes, as described in the HIPAA Privacy Rule. The DURSA, however, further restricts when UConn Health may send or receive PHI via the Exchange without an authorization for payment or health care operations purposes. The following Guidelines are intended to address these additional restrictions under the DURSA.

B. Guidelines

1. UConn Health may request, retrieve and send data via the Exchange for uses and disclosures pursuant to an authorization from the patient (or the patient's authorized representative) that complies with HIPAA and other applicable laws, regulations and UConn Health policies.

2. In the absence of a valid authorization from the patient/authorized representative:

    a. UConn Health may request, retrieve and send data via the Exchange for treatment of the individual who is the subject of the data.

    b. UConn Health may request, retrieve and send data via the Exchange for the payment activities of a health care provider for the individual who is the subject of the data.

    c. With respect to information that UConn Health *sends* to another party via the Exchange, UConn Health may further request, retrieve and send such data via the Exchange for its own "health care operations," as defined under HIPAA.

    d. With respect to information that UConn Health *retrieves* from the Exchange, UConn Health may further request, retrieve and send such data via the Exchange for only the following health care operations of UConn Health:

        i. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. § 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

        ii. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

        iii. Health care fraud and abuse detection or compliance; and

iv. Public health activities and reporting as permitted by the HIPAA Privacy Rule (45 C.F.R. §§ 164.512(b) and 164.514(e)) and other applicable law.

e. UConn Health may request, retrieve and send data via the Exchange for any purpose to demonstrate meaningful use of certified electronic health record technology, as further described in the DURSA.

Questions concerning these Guidelines should be directed to the UConn Health Director of IT Security and/or the UConn Health Office of the General Counsel.