

Report on Patient Privacy Volume 22, Number 2. February 10, 2022 Safeguards in New National Network Include Insurance, App Mandates, Cybersecurity Council

By Theresa Defino

The new national health information network calls for a number of privacy and security safeguards and standards that, in some instances, exceed what HIPAA covered entities (CEs) and business associates (BAs) are required to meet under current federal regulations.

For example, qualified health information networks (QHINs) that join the national one will have to maintain a certain level of cyber insurance, and obtain certification by a nationally recognized security framework, such as the HITRUST. In addition, organizations such as health apps that join the network that aren't now defined as CEs will find they have to comply with breach or security incident notification and other requirements that mimic HIPAA.

After years in development, last month officials with the HHS Office of the National Coordinator for Health Information Technology (ONC) and the Sequoia Project, its recognized coordinating entity (RCE), announced the Trusted Exchange Framework and Common Agreement (TEFCA).^[1] Together they will underpin a national, interoperable health information network, composed itself of QHINs. Interested organizations may apply to be QHINs within the coming months, with the network itself expected to be rolled out over the next few years.

ONC made it clear to the Sequoia group that "privacy and security" were to be a "huge focus area" in TEFCA, Sequoia CEO Mariann Yeager told *RPP* in an interview. Along with feedback from stakeholders, there was a "consistent sentiment that there should be a high bar for privacy and security for QHINs, given the role that they would play as really part of a national backbone," Yeager said.

She added that the Common Agreement "expects covered entities and business associates to continue to meet their obligations under HIPAA and comply with applicable law," but certain HIPAA-like standards will now be imposed on "entities that are not subject to HIPAA that are parties to the exchange."

The Trusted Exchange Framework "is a set of non-binding principles to facilitate data-sharing among health information networks," ONC Director Micky Tripathi and Yeager wrote Jan. 18 on the ONC blog.^[2] The Common Agreement "will operationalize simplified electronic health information exchange for many across the US and will provide easier ways for individuals and organizations to securely connect."

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)