

Report on Patient Privacy Volume 20, Number 2. February 06, 2020 Amid Release of Framework, HHS Pledges Access to Records, Privacy, Interoperability

By Theresa Defino

The year is still young, but the federal government has announced a potentially far-reaching privacy effort that should catch HIPAA compliance officers' attention. And HHS Secretary Alex Azar, speaking at the recent annual meeting of the Office of the National Coordinator (ONC) for Health Information Technology, signaled^[1] his department's intention to push forward with the administration's efforts to make medical records access easier for patients and to increase interoperability of electronic health records (EHRs).

Likely of most immediate interest is the first (but finalized) version of the "National Institutes of Standards and Technology Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management," which NIST officials were "thrilled" to announce on Jan. 16.^[2] Although NIST is part of the Department of Commerce, not HHS, the agencies have closely collaborated on a number of projects. Each year, for example, the Office for Civil Rights (OCR) and NIST cosponsor an annual cybersecurity conference.

The privacy framework is meant to be complementary to NIST's Cybersecurity Framework, first issued in February 2014 and updated in April 2018. The Cybersecurity Framework consists of five concurrent and continuous functions that constitute the cybersecurity life cycle for any organization: identify, protect, detect, respond and recover. In the privacy framework, the corollaries are identify, govern, control and communicate.

The framework is designed to help the U.S. "data-driven economy" with its "tricky balancing act": "building innovative products and services that use personal data while still protecting people's privacy," NIST said in its announcement. The draft framework was issued in September.

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

[Purchase Login](#)