COSMOS
Navigate the Compliance Universe

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.

As NIST explained, "The Privacy Framework approach to privacy risk is to consider privacy events as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal. The Privacy Framework describes these data operations in the singular as a data action and collectively as data processing. The problems individuals can experience as a result of data processing can be expressed in various ways, but NIST describes them as ranging from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm."

Those who may have implemented, or are familiar with, the draft framework will find much unchanged. As NIST explained, "as with its draft version, the Privacy Framework centers on three sections: the *Core,* which offers a set of privacy protection activities; the *Profiles,* which help determine which of the activities in the Core an organization should pursue to reach its goals most effectively, and the *Implementation Tiers,* which help optimize the resources dedicated to managing privacy risk."

NIST said the framework "based on nearly a year of extensive public conversations...provides guidance for organizations that need to develop strategies to minimize privacy risks while still accomplishing their missions. It also provides a way for organizations to have productive dialogues about privacy risks arising from their products or services."

Framework a 'Valuable Resource'

Karen Greenhalgh, managing principal and founder of the consulting firm Cyber Tyger, tells *RPP* that there are "few" differences between the draft and the finalized version, but these include improvements, as detailed in the framework, that "substantiate the input of the many healthcare professionals involved in the development process."

Employing an "outcome-based methodology," says Greenhalgh, the framework "addresses privacy as a measurable risk, enabling privacy practitioners to state goals with measurable outcomes. Communication to document and measure achievable goals will be particularly helpful to the health care industry."

She adds that NIST mapped the privacy framework to the cybersecurity framework, as well as to additional guidance from NIST, including its risk management framework. The new framework, says Greenhalgh, is made more effective as a result of industry input.

"Health care has specific privacy and security concerns that do not exist in other industries, and as a critical infrastructure, those needs must be addressed. The representation of health care privacy professionals in the development of the Privacy Framework makes it a valuable resource for the entire industry," she tells *RPP.*

Azar: Status Quo 'Fiercely Defended'

Speaking during his keynote address at ONC's annual meeting, this year titled "Connecting Policy and Technology: Bringing the EHR to the Patient,"Azar recalled his frustration and a host of failed attempts to obtain his own medical records.

Earlier in January, he "spent hours trying unsuccessfully to get access into my health records," and as of his Jan. 27 remarks, Azar said he hadn't even gotten a call back "to help me get into them." He joked that this was occurring despite his position. "There was no preferential treatment, just equal opportunity frustration."

Azar added that, in 2019, "I had to visit three different providers that were all part of the same large system: a primary care practice, an imaging provider, and an inpatient hospital. Yet each of them had a separate system—within this one business, they didn't even have interoperability! And this isn't just frustrating. Each of these issues is an opportunity for medical error."

Last year, HHS published[3] two related proposed rules, both of which Azar reiterated support for.

ONC's draft regulation requires health care providers and others to cease practices the government is calling "information blocking," or face fines or possible exclusion from government health programs. It offered seven exceptions for when blocking is permitted, including "promoting the privacy of electronic health information." The Centers for Medicare & Medicaid Services published a corresponding proposed rule.

Azar said the ONC rule, required under the 21st Century Cures Act, "may be complex, but the goal is very simple: It's about access and choice. Patients should be able to access their electronic medical record at no cost, period," and he acknowledged that the proposed rule has faced opposition.

"Unfortunately, some are defending the balkanized, outdated status quo and fighting our proposals fiercely," Azar said.

OCR has already tried to make the point with covered entities and business associates that it expects compliance with the access requirements, including price and timing.

Last year, for the first time, OCR entered settlement agreements over alleged HIPAA violations related to records access; both cases were with providers in Florida that each separately agreed to an $85,000 payment and one-year corrective action plan. OCR's efforts faced a setback last month, however, when a judge invalidated price limits when applied to records patients authorize to be sent to third parties.[4]

Azar added that HHS's interoperability and health information technology efforts are "beyond control of clinical records. Putting patients in charge of their health records is a key piece of patient control in healthcare, and patient control is at the center of our work toward a value-based healthcare system."

Azar did not indicate when the final interoperability rule will be published. Following a review of some 2,000 comments, the final rule has been under review by the Office of Management and Budget since Oct. 28, 2019.

The government is continuing to meet with stakeholders concerning the rule, as evidenced by entries on reginfo.gov.[5]

Contact Greenhalgh at karen@cybertygr.com.

[1] HHS Secretary Alex Azar II, "Remarks at the 2020 ONC Annual Meeting," January 20, 2020, http://bit.ly/2RQnsC5.
[2] National Institute of Standards and Technology, "NIST Releases Version 1.0 of Privacy Framework," January 16, 2020, http://bit.ly/3b1r8Z7.
[3] Theresa Defino, "With New Proposed Rule, HHS Seeks to Halt 'Nefarious' Blocking of Electronic Health Info," *Report on Patient Privacy* 19, no. 3 (March 2019), http://bit.ly/37sqD8i.
[4] Theresa Defino, "Judge Invalidates OCR's Third-Party Requirements Under Access Rights,"*Report on Patient Privacy* 20, no. 2 (February 2020).
[5] Office of Information and Regulatory Affairs, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, Executive Order 12866 meetings, http://bit.ly/3b7ggc7.