Health Care Alert: Senate Panel Hears Concerns that ONC's Proposed "Interoperability" Rule Could Expose New Cybersecurity Risks; Comments Due May 3, 2019

Related Industries

Health Care

CLIENT ALERT | 3.27.2019

On March 26, 2019, the U.S. Senate Committee on Health, Education, Labor & Pensions held a hearing to evaluate a rule proposed by the Office of the National Coordinator for Health Information Technology (the ONC) to implement certain provisions of the 21st Century Cures Act (the Act) related to health information technology (health IT).

The rule proposes a number of revisions to the criteria for certification under the ONC Health IT Certification Program (the Program), including a new "Application Programming Interfaces" (API) criterion. Generally, APIs enable third-party software developers to create programs and applications that interact with the certified IT, and the proposed rule seeks to promote interoperability and innovation by requiring developers of certified health IT to use specific standards and implementation specifications already established in the industry (specifically, the Health Level 7 Fast Healthcare Interoperability Resources, or FHIR® standards). Several witnesses voiced concerns that third-party developers may not be subject to the privacy and security standards of the Health Insurance Portability and Accountability Act (HIPAA), and further that the rule does not contemplate any process to vet such developers for cybersecurity risks.

The proposed rule also sets forth seven exceptions from the definition of unlawful "information blocking," defined in the Act to include practices by health IT developers, health information exchanges and networks, and health care providers that are likely to "interfere with, prevent, or materially discourage" the access, exchange, or use of EHI.[1] The exceptions to this broad definition may be crucial for providers, as the Act authorizes the Department of Health and Human Services' Office of Inspector General (OIG) to impose civil monetary penalties of up to $1,000,000 for information blocking violations. While the Act states that a health care provider may be found liable for information blocking only if the provider "knows that [its particular information blocking] practice is unreasonable,"[2] at least one witness expressed concerns that providers lacking the resources or expertise to appropriately address the interoperability limitations of their health IT

could still be exposed to significant liability risk.

Specifically, the proposed rule would exclude the following "reasonable and necessary activities" from the definition of "information blocking," so long as the developer, exchange, network, or provider is able to satisfy all requirements of the applicable exception:

- **Preventing harm**, in accordance with the requirements of proposed 45 C.F.R. § 171.201;
- **Promoting the privacy of EHI**, in accordance with the requirements of proposed 45 C.F.R. § 171.202;
- **Promoting the security of EHI**, in accordance with the requirements of proposed 45 C.F.R. § 171.203;
- **Recovering costs reasonably incurred**, in accordance with the requirements of proposed 45 C.F.R. § 171.204;
- **Responding to requests that are infeasible**, in accordance with the requirements of proposed 45 C.F.R. § 171.205;
- **Licensing of interoperability elements on reasonable and non-discriminatory terms**, in accordance with the requirements of proposed 45 C.F.R. § 171.206; and
- **Maintaining and improving health IT performance,** in accordance with the requirements of proposed 45 C.F.R. § 171.207.

The full text and preamble of the proposed rule were published in the Federal Register on March 4, 2019, and are available here. If you have questions about the rule's provisions, their expected impact, or the process to submit your comments, please contact Jonathan Ishee, Nita Garg, Mairi Mull, or your regular Vorys attorney.

--

[1] 42 U.S. Code § 300jj–52(a)(1).

[2] *Id*.