Jill DeGraff
Founder and Managing Member
1875 Connecticut Avenue, NW 10th Fl
Washington DC 20009
JDeGraff@ApertureLaw.Group

June 3, 2019

--submitted electronically via http://www.regulations.gov --

Donald Rucker, MD
National Coordinator for Health Information Technology
U.S. Department of Health & Human Services
330 C Street SW, Floor 7
Mary Switzer Building
Washington, D.C. 20201

Re: 21st Century Cures Act: Interoperability, Information Blocking and the ONC Health IT Certification Program Proposed Rule – Information Blocking – Promoting Privacy (Section 171.202)

Dear Dr. Rucker,

I appreciate the opportunity to comment on the proposed rules for data interoperability, information blocking and the ONC's health IT certification program.

I counsel HIPAA covered entities and vendors of healthcare technologies on privacy, data security and contracts. This vantage point gives me a point of view about consumer privacy and data portability. I would like to offer my comments on the information blocking rule, particularly in regard to the "promoting privacy" exception and, more broadly, the policies that give effect to the individual right of access under HIPAA.

The HIPAA Privacy Rule and Data Portability Between Covered Entities

The HIPAA Privacy Rule includes detailed specifications that govern the permissible disclosure of PHI between covered entities, but it does not affirmatively require these disclosures to be made. This is a critical juncture where data portability gets stuck. The information blocking rule fills a critical gap in the HIPAA Privacy Rule, by inducing health care providers and their respective supply chains to facilitate data portability with other HIPAA covered entities, or else face negative consequences under the enforcement authorities granted by Congress to the ONC and the OIG in the Cures Act.

Individual Right of Access

Other commenters have expressed concern that the proposed rules will increase privacy risks and opportunities for consumer fraud. They urge caution about policies that position consumers as "mediums to a vast, yet nascent ecosystem of clinician, researcher and patient-facing apps, which rely

upon newfound access to data produced and retained by certified health IT."[1] They expect that Congress will need to step in to fill the gaps in consumer protection "residing just beyond the reach of HIPAA".

While I appreciate these concerns, I'd like to address them within the broader context of consumer privacy laws. Privacy law always involves a balancing of public and individual interests. Weighing privacy risks and opportunities for consumer fraud is part of this balancing exercise. In the end, consumers are best positioned to evaluate how these interests should be weighed, with the signals presented to them about a service provider's privacy practices. Having a "no wrong door" policy for consumer-initiated requests to port medical records is the ultimate expression of consumer protection, especially when these interests can shift when a medical emergency arises.

Public benefits from expanded competition is another consideration in the balancing of public and individual interests. Competition from all corners of the digital ecosystem is needed to inspire innovation within the U.S. health system. Imagine a business case where a health care provider gives her patients a mobile app. The mobile app allows her to designate the provider as the holder of record for her medical records. The app uses this authority to query other health care providers, health information networks and health for medical record updates. Patient loyalty ensures. While developers on either side of the HIPAA divide may be able to deliver these features and functionality, data portability and access to competitive technologies and services offers health care providers an opportunity to compete for their patients' loyalty over other health care providers. Without robust competition, health care providers may be less inspired to innovate.

Another part of considering the context is illustrated by the increased activism in consumer privacy across industry sectors, exemplified by the E.U. General Data Protection Regulation, the California Consumer Privacy Act of 2018, and privacy proposals circulating in multiple state legislatures and Congress. This activism is generating consensus for an expanded conception of privacy that elevates individual rights, improves transparency about privacy practices, expands user controls regarding data use and sharing, and addresses consumer rights of access, deletion and portability. If these legislative trends continue, the consumer protections "just beyond the reach of HIPAA" should fall into closer alignment with HIPAA. This will be an encouraging development for consumers, who don't concern themselves the way privacy practitioners do with where HIPAA's outer perimeter is drawn.

Another touchpoint in the broader context of consumer privacy relates to a shift in business mindset. Instead of treating personal information as business records, more businesses are starting to realize that their privacy practices should align with their business values, and that their business values should align with consumer values. Integrating formal privacy risk assessment into their business practices and culture is how they can bring this alignment together. This will have profound consequences for data governance, especially in businesses that deliver software-as-a-services with capabilities enabled by big data, deep learning and automation. As some providers deliver increasingly sophisticated services involving the use and sharing of their health information, it will become easier to distinguish the businesses that only talk about their privacy values from businesses that live their privacy values.

This brings us to another area of innovation in the wider privacy conversation: Privacy-by-design. Increasingly, the conversation addresses the need to supplement the prevalent notice-and-consent-

[1] Letter to the ONC from the American Medical Informatics Association, dated May 23, 2019, accessed on June 3, 2019 at https://uploads.strikinglycdn.com/files/e3194a19-5d5a-4069-9714-f2d2f725fa6d/AMIA%20Response%20to%20ONC%20Cures%20NPRM_vfinal.pdf?id=170072

model with “privacy-by-design” standards. Some of these standards have already been codified through self-regulating, voluntary codes of conduct, including the Digital Advertising Alliance’s recently updated its Code of Conduct and the CARIN Alliance’s proposed Code of Conduct. The DAA Code of Conduct is notable for detailed guidance it provides for health information, including robust consent at the point of collection and additional opt-out/opt-in rights related to data sharing. The CARIN Alliance Code of Conduct is at an earlier stage in its maturity (the first DAA Code of Conduct was released in 2003, while the CARIN Alliance Code of Conduct was first released in fall 2018), but its scope is squarely aimed at software developers who support the delivery of services to consumers using PHI brought from the HIPAA-regulated environment under the HIPAA individual right of access. DAA and The CARIN Alliance’s respective codes of conduct illustrate the possibility for a secondary market of endorsement organizations, which would produce additional signals to inform consumer preferences. Over time, deeper consensus may emerge around detailed requirements to address a multiplicity of common scenarios that require a specialized balancing of public and individual interests, which is something that the HIPAA Privacy Rule is exceptionally well-equipped to do. These efforts could eventually lead to an industry-recognized standard for privacy practices, comparable to ISO 18001, NIST 800-53 or AICPA Trust Principles for data security, which could lead to even more companies adopting privacy practices that further mitigate privacy risks and opportunities for consumer fraud.

While it takes time for a privacy ecosystem of consumer protections for health information to develop outside of the HIPAA-regulated environment, I don’t recommend that you wait for this ecosystem to mature. If you did, who would get to decide when it is sufficiently mature? What would be the criteria to decide when it is? How much iterative consultation with stakeholders would be needed before making the decision? Waiting for the ecosystem to mature will thwart innovation, and slow the progress of innovations that put health and medical information where it needs to be, at the time when it’s needed, both within consumer’s own workflows and within the health IT infrastructure globally.

In summary, while the privacy risks and opportunities for consumer fraud are valid concerns, they need to be considered in relation to other public and private interests. To me, the ONC strikes the right balance.

Sincerely,

Jill DeGraff
Managing Member
Aperture Law Group PLLC