Congressional Issue Brief: Individual Health Data Access

Overview

For more than twenty years, Congress has prioritized individuals' access to their health information as a key lever to improve care, enable research, and empower Americans to live healthy lifestyles. But across the paper-based world of HIPAA to the digital aspirations of 21st Century Cures, the ability of individuals to access and use their health information continues to be a challenge. While Congress has passed, and HHS has implemented, a host of policies and programs to improve patient data access, patients continue to struggle to have access to their health information. Meanwhile providers and other health professionals face mounting challenges in managing patient health information and easily fulfilling patients' information requests.

The "P" Stands for Portability

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, a patient has the right to access their protected health information (PHI) in one or more "designated record sets" maintained by a covered entity in the form, format, and manner requested if readily producible.[1] The designated record set (DRS) is defined as a group of records maintained by or for a covered entity that comprises the: "(1) medical records and billing records about individuals maintained by or for a covered healthcare provider; (2) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, or (3) other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals."[2]

The Privacy Rule further states that the term "record" refers to "any item, collection or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity."[3]

Guidance released by the HHS Office for Civil Rights in 2016 known as the "HIPAA Access Guidance" sought to further illuminate what types of information could be considered part of the DRS stating that, ". . . individuals have a right to a broad array of health information about themselves maintained by or for covered entities including: medical records, billing and payment records; insurance information; clinical laboratory test results; medical imaging, such as X-rays, wellness and disease management program files, and clinical case notes; among other information used to make decisions about individuals."[4]

Given the broad nature of HIPAA's definition and HIPAA-related guidance, healthcare organizations have interpreted differently and applied inconsistently which information may be included as part of the DRS. This variation has led to discrepancies in the information provided to patients regarding the medical records release process and confusion over how to comply with

federal and state regulations and recommendations among some of the nation's most highly ranked hospitals.[5]

HITECH: Adapting HIPAA for The Digital Age

Today, defining the DRS is further complicated because electronic health record (EHR) systems often have different designs, functions, data structures, and interfaces.

When HIPAA was enacted in 1996 only a handful of hospitals and virtually no physicians used EHRs. A decade later, EHR use was meager with less than 15 percent of hospitals using them. This adoption curve saw a dramatic uptick due to the Health Information Technology for Economic and Clinical Health (HITECH) Act which offered $34 billion in incentives for hospitals and physicians to adopt EHRs as part of the American Recovery and Reinvention Act of 2009. The HITECH Act also extended the HIPAA right of access by granting individuals an explicit right to an electronic copy of their health information.[6]

Despite this affirmation of HIPAA's right of individual access in a digital world, this policy needed technical specifications and a regulatory schema to be operationalized. To do this, the HITECH Act established the Office of the National Coordinator for Health IT (ONC) to oversee development of a nationwide health IT infrastructure, including health IT standards, implementation specifications, and certification criteria for EHRs. Initially established to support the EHR Incentive Program, ONC published a preliminary set of certification criteria in 2011 and updated these technical specifications in 2014, establishing functionality beyond the Incentive Program.

Relevant to advancing patient data access, the EHR Incentive Program required hospitals and physicians to provide patients with online access to specific data types, including medications, lab results, problem lists, and immunization information, among others. Over time, these hospital and physician office patient portals were required to allow individuals the functionality to "view, download, and transmit," to a third party their health information to receive incentive payments (and currently avoid penalties).

The 2015 Edition Health IT Certification Criteria (2015 Edition) final rule[7] built upon previous rules developed by ONC to facilitate EHR interoperability and enable health information exchange. The 2015 Edition adopted the Common Clinical Data Set (CCDS) definition, which was an outgrowth of the initial "Meaningful Use Common Dataset" that ONC adopted in 2012. The CCDS included new and updated vocabulary and content standards for clinical data exchange, including: immunizations, unique device identifiers (UDIs), assessment and plan of treatment, goals, and health concerns.[8] It also further expanded the accessibility and availability of data exchanged by including enhanced data export and application programming interface (API) capabilities, all of which required that at a minimum the CCDS be available.

While the 2015 Edition made available an expanded set of data through certified EHRs for Patient Data Access, the CCDS falls well short of all data within a patient's EHRs and is exceptionally short of what any given hospital's DRS might include.

Curing Patient Data Access Woes

Congress sought to address a host of complaints related to EHR interoperability and further broaden what data should be available for patients to access in 2016. The 21st Century Cures Act sets an expectation that all patient health information stored electronically will be able to be exchanged. Specifically, Cures defines interoperability in the context of health IT that (1) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;[9] (2) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law;[10] and (3) does not constitute information blocking.[11]

In January 2018, ONC announced a draft policy known as the US Core Data for Interoperability, or USCDI. The USCDI intends to build upon the CCDS definition and "provides the process, data policy context, and structure by which a predictable schedule to expand the USCDI can be accomplished through collaboration with the industry," so that ONC can "support the Cures Act requirement of all electronic health information from a patient's record being available."[12]

Cures also established the NIH Precision Medicine Program, known as the All of Us Research program, which will enable more than 1 million Americans to donate their health data for research. The mechanism through which patients are donating their data is known as Sync 4 Science (S4S).[13] The technical specifications developed for the NIH through S4S give providers a HIPAA-compliant way to enable patients to participate in research studies while eliminating use of staff and other resources to satisfy patient requests for medical record data requests. Under the program, patients data requests and delivery are self-provisioned through the healthcare provider's vendor-supplied EHR patient portal.[14]

In combination, these policies should help deliver on the rights granted to patients under HIPAA in an increasingly data-centric world through EHRs and other health IT. But just because Congress says it must be so, does not mean it is so.

Looking Ahead

In 2017, over half (52%) of individuals were offered access to an online medical record by a provider or insurer, according to government data.[15] However, patients continue to struggle in obtaining copies of their records[16],[17] and providers are incumbered in delivering them to patients in a complete and timely fashion due to the complexity of finding, managing, and delivering information requests.[18]

While numerous administrative policies launched in the last year have prioritized Patient Data Access, most of these policies either need more definition or they need to be further translated into regulation and – equally – put into practice. Specifically, the CMS MyHealthEData initiative and Cures provisions have not been translated into actionable or enforceable policy. Furthermore, ONC has not finalized provisions related to the use of APIs "without special effort," nor has it provided technical specifications for how health IT must allow for "complete access, exchange, and use of all electronically accessible health information," or has it released its policy on "information blocking." While CMS has finalized recent changes to the Promoting Interoperability Program for hospitals

and physicians to facilitate patient access to their data via patient portals – and increasingly through APIs – these policies pertain only to the limited CCDS and will not begin until 2019.

It is possible that existing policy and strategy needs refinement. There has been a long-standing discordance between what federal policy requires and what technology and/or organizational policies have delivered as part of HIPAA's individual right of access. HIPAA established broad definitions and these concepts were developed long before use of EHRs, mobile apps, and other kinds of health technology became commonplace. In a document-centered, paper-based world, defining information in terms of "records" makes sense, but as nearly 98 percent of all discharges in the US were made using EHRs, we must rethink how to better ensure individuals' right of access in a data-centric world.

References

[1] Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, Subparts A and E.
[2] HIPAA Individual Right of Access Guidance available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.
[3] Id.
[4] Id.
[5] Lye CT, Forman HP, Gao R, et al. Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records. *JAMA Netw Open*. 2018;1(6):e183014. doi:10.1001/jamanetworkopen.2018.3014
[6] Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5. 123 Stat. 268. February 17, 2009.
[7] 80 FR 62601, 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications, https://www.federalregister.gov/documents/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base
[8] 2015 Edition Certification Companion Guide. https://www.healthit.gov/sites/default/files/2015Ed_CCG_CCDS.pdf
[9] Cures Sec. 4003(a)(2)
[10] Id.
[11] Id. Ref. Section 3022(a).
[12] Office of the National Coordinator for Health IT. USCDI Draft Policy.
[13] http://syncfor.science/
[14] Id.
[15] Individuals' Use of Online Medical Records and Technology for Health Needs, ONC Data Brief, No. 40, April 2018.
[16] Lye CT, Forman HP, Gao R, et al.
[17] Murphy-Abdouch K. Patient access to personal health information: regulation vs. reality. *Perspect Health Inf Manag*. 2015;12(winter):1c.
[18] Fioriglio G, Szolovits P. Copy fees and patients' rights to obtain a copy of their medical records: from law to reality. *AMIA Annu Symp Proc*. 2005;2005:251-255.