Issue Brief
Align HIPAA 'Right of Access' with ONC Health IT Certification Functionality

Problem

For more than twenty years, Congress has prioritized individuals' access to their health information as a key means to improve care, enable research, and empower Americans to live healthy lifestyles—from the paper-based world of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to the digital aspirations of the 21st Century Cures Act of 2016 (Cures). However, individuals' ability to access and use their health information continues to be a challenge.

There remains a fundamental disconnect between what the HIPAA right of access requires and what Certified Health IT can deliver. This disconnect between policy and functionality places both clinicians and patients in an untenable position, especially as mounting volumes of data from an endless number of sources—from the human genome to wearables—makes the challenge of providing patients access to their health information more difficult. Policymakers must modernize HIPAA so that the Office of the National Coordinator for Health IT's (ONC's) Certification Program can support the HIPAA right of access.

Background: Designated Record Set

Under the HIPAA Privacy Rule, a patient has the right to access their protected health information (PHI) in one or more "designated record sets" (DRSs) maintained by a covered entity in the form, format, and manner requested if readily producible.[1] The 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]

While healthcare organizations are generally tasked with defining the types of documentation that comprise the DRS, guidance released by the U.S. Department of Health and Human Services' 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. It states 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 and confusion, even among some of the nation's most highly ranked hospitals, in the information provided to patients regarding the medical records release process.[5]

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

Background: Health IT Certification

When HIPAA was enacted in 1996, only a handful of hospitals and virtually no physician offices 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 with enactment of 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 Reinvestment 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 individual right of access in a digital world, this policy needed technical specifications and a regulatory schema to be operationalized. To do this, the HITECH Act formally established into law the Office of the National Coordinator for Health IT to oversee development of a nationwide health IT infrastructure, including health IT standards, implementation specifications, and certification criteria for EHRs. ONC published a preliminary set of certification criteria in 2011 to support the EHR Incentive Program, and it updated these technical specifications in 2014.

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, hospital and physician offices' patient portals were required to allow individuals the functionality to "view, download, and transmit," to a third party their health information in order to receive incentive payments (and currently avoid penalties). The introduction of this functionality would set the stage for functionality that was not yet widespread, and it would further engrain patients' expectations for access to their data.

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.[9]

While the 2015 Edition made available an expanded set of data through certified EHRs for Patient Data Access, the CCDS and the proposed U.S. Core Data for Interoperability (USCDI) standard fall short of all data within a patient's EHR and are exceptionally short of what any given hospital's or physician's DRS might include.

The proposed ONC information blocking rule also seeks to adopt a new 2015 Edition certification criterion that requires health IT developers to have the capability to enable a healthcare provider, his or her office staff, or a software program to electronically export all electronic health information they "produce and electronically manage in a computable format" for a single patient when a patient submits a valid HIPAA right of access request.[10] While the definition of "electronic health information" as proposed under the rule will likely dramatically expand the universe of electronic health information available, not all information that must be provided to a patient as part of the DRS under HIPAA resides within the EHR, such as imaging, nuanced progress notes, and legacy system information about the patient.

Recommendations for Aligning HIPAA with Health IT Certification

Inconsistencies in concepts and terminologies have hampered individuals' right of access, and the broad definition of the DRS has made it difficult to operationalize in practice. AMIA and AHIMA recommend that policymakers take concerted action to align HIPAA's right of access with Health IT certification so individuals can view, download, or transmit this information electronically to a third party and access the information via application programming interfaces (APIs).

Specifically, we recommend lawmakers revise the definition of the DRS and require certified Health IT to provide the amended DRS to patients electronically while maintaining computability. Further, regulators should develop guidance and request regular feedback from stakeholders on continued barriers to delivering this right under HIPAA. This revision would provide greater clarity and predictability of what constitutes the DRS to both providers and patients.

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] Ibid.
[4] Ibid.
[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] Under the recently released information blocking rule, ONC has proposed replacing the CCDS with the United States Core Data for Interoperability (USCDI) standard—a modest expansion of the CCDS that specifies a common set of data classes for clinical data exchange including: pediatric vital signs, clinical notes, and provenance—(i.e.—metadata or extra information about data that can answer such questions as who created the data or when.)
[10] Available at: https://www.healthit.gov/sites/default/files/nprm/ONCCuresActNPRM.pdf.