FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW
WASHINGTON HARBOUR
3000 K STREET, N.W.
SUITE 600
WASHINGTON, D.C. 20007-5109
202.672.5300 TEL
202.672.5399 FAX
WWW.FOLEY.COM

WRITER'S DIRECT LINE
202.945.6119
dromano@foley.com EMAIL

CLIENT/MATTER NUMBER
117431-0101

January 28, 2019

Don Rucker, M.D.
National Coordinator for Health IT
Office of the National Coordinator
U.S. Department of Health and Human Services
330 C Street SW
Mary Switzer Building; Office 7009A
Washington, D.C. 20201

RE: Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs

Dear Dr. Rucker:

On behalf of Ciox Health, LLC ("Ciox Health"), Foley and Lardner LLP is pleased to submit comments on ONC's draft strategy for reducing regulatory and administrative burden. We appreciate the significant effort ONC put into developing the strategy as well as the collaborative nature of the strategy. Reducing burden on our nation's clinicians will require all HHS agencies working together to address the regulatory burdens imposed by the many rules and guidance documents that all too often force clinicians to focus more on paperwork than patients. We appreciate the opportunity to provide feedback on the draft strategy and look forward to working with ONC to ensure that the final strategy addresses the wide breadth of burdens clinicians face that were highlighted in the 21st Century Cures Act.

Introduction

Ciox Health is a health technology company working to solve the clinical data liquidity challenge, providing transparency across the healthcare ecosystem and helping clients manage disparate medical records. When stakeholders do not have timely access to the complete clinical picture of patients, critical decisions about patient care, medical outcomes research, disease prevention, reimbursement, and payments are negatively affected. Ciox Health's scale, expertise, expansive provider network, and industry-leading technology platform make it the most reliable clinical data company in the United States. Ciox Health partners closely with health systems and providers to ensure they are interoperable, and they can meet their release of information requirements and provide patients with access to their health information. Ciox Health processes the

retrieval of 100 million records annually. Through its standards-based technology platform, HealthSource, Ciox helps clients securely and consistently solve challenges in clinical interoperability.

Section 4001 of the 21st Century Cures Act (the "Cures Act") added section 13103 to the Health Information Technology for Economic and Clinical Health Act (HITECH), which acknowledged that all too often clinicians are being forced to prioritize paperwork over patients and that physicians on average are facing higher burnout rates as regulatory and administrative requirements have increased over time. Although there are many reasons for the increase in clinician burden, section 13101 identified a number of areas of particular concern related to the use of health IT and EHRs, and directed ONC to develop a strategy to address these burdens. In particular, section 13101 identified the following as priority areas: (1) "incentives for meaningful use of certified EHR technology for eligible professionals and hospitals;" (2) "activities that provide individuals access to their electronic health information;" and (3) "activities related to protecting the privacy of electronic health information."[1] Although we agree with the burdens identified in the draft strategy, and generally agree with ONC's recommendations to address those burdens, we believe that ONC has overlooked a few significant burdens facing providers on a daily basis that the Cures Act specifically asked ONC to address.

The Health Insurance Portability and Accountability Act (HIPAA) established the fundamental right for individuals to have easy access to their health data, so that they could participate in the management of their health and wellness as well as the health and wellness of those for whom they are caregivers. The purpose of this right was to improve patients' health. We strongly believe in this fundamental right and that interoperability is a necessary underpinning to making data easily accessible to patients and caregivers.

We are encouraged by the industry's adoption of the Consolidated Clinical Document Architecture (C-CDA) to share summary of care documents with patients and the emerging adoption of Fast Healthcare Interoperability Resources (FHIR) application programming interfaces (APIs) that make it easier for patients to use the application (app) of their choosing to access their electronic health information for patient treatment. Although such technologies are not designed to address the totality of a patient's protected health information (PHI), their eventual adoption will facilitate the exchange of appropriately limited and useful electronic data, known as the Common Clinical Data Set (which ONC is proposing to rename to the U.S. Core Data for Interoperability (USCDI)). We support such developments and policies which encourage the goal of interoperability. In the meantime, Ciox Health's more than 40 years of experience with records management and release of information requests have demonstrated that there is a significant difference in the burden placed on clinicians and their organizations to provide the USCDI versus the larger designated record set as

[1] 21st Century Cures Act (Pub. L. No. 114—255) at https://www.gpo.gov/fdsys/pkg/PLAW-114publ255/pdf/PLAW-114publ255.pdf.

defined in HIPAA, and this distinction needs to be carefully maintained and unintended consequences must be managed closely.

Whereas the USCDI from a single, adequately configured, certified EHR can be provided in electronic format in accordance with the terms of section 13405(e) of the HITECH Act with relative ease, this is not the current reality of the interoperability landscape. Requests for medical information from patients and third parties often are for the entire designated record set, and often span multiple settings of care and multiple EHRs (both certified and not certified). These requests routinely ask for production in paper format, even when the record being requested is maintained as part of an EHR. Additionally, these requests often ask for data that is part of the USCDI, but is not populated in a C-CDA or FHIR API because health systems have not configured their systems to include it. It is incredibly burdensome and time consuming to retrieve and provide the larger designated record set for these requests. With the average hospital using 16 different EHRs, paper-based records, offsite storage, and microfiche, it can take hours, days or even weeks of work to put together a response to a single patient's designated medical record set. These requests become even more burdensome when the provider is directed to produce the entire set in paper format. Unfortunately, existing regulations and guidance have failed to acknowledge any variance between the effort required to produce the USCDI from a certified system in electronic format versus the entire designated record set (again, often in paper format). *This lack of precision has created a significant regulatory burden for healthcare organizations (costing them more than $1.5 billion per year and over $22 billion in lifetime regulatory costs) and ultimately threatening the privacy of patients' data.*[2]

Discussion

A. The rules have failed to recognize the distinction between (1) the patient and personal representative who are using the data to manage the patient's health and (2) other parties who are using the data for other purposes, including attempting to monetize the data for commercial gain. This distinction must be restored and maintained for several important reasons that are described here.

To ensure patients have easy access to their data, the HIPAA Privacy Rule limited the fees that providers can charge individuals for copies of their own records to the labor costs for copying and the cost of supplies. The rules do not allow for the recovery of other costs, such as those incurred for record search, retrieval, handling, and ensuring compliance. Additionally, the Privacy Rule did not account for or allow for any fees related to the technical infrastructure necessary to make data electronically available to patients (i.e. the cost of servers, the cost to maintain APIs, the cost to update software). The HITECH Act further specified that when a covered entity uses an

[2] "Broad Patient Directive and February OCR Guidance May Trigger a $1.52 Billion Cost Shift to Providers." Leavitt Partners ("Leavitt Report").

EHR, individuals have the right to get a copy of their health information contained in that EHR in an electronic format and to have it sent directly to a third party (person or entity) electronically. It also again limited the fees chargeable to individuals for requesting such data to labor costs only. HITECH does not, however, apply such limitations to data sent to a third party pursuant to a patient directive.[3]

HHS promulgated regulations in 2013 (the "2013 Omnibus Rule) to, among other things, implement the HITECH Act amendments to HIPAA. Then, in 2016, it issued sub-regulatory guidance via FAQs (the "2016 Guidance") with the intent of further clarifying and implementing HITECH. Regrettably, the 2013 Omnibus Rule and the 2016 Guidance exceeded the HITECH requirements in a few ways. First, the 2013 Omnibus Rule applied the HITECH requirements not only to electronic health information kept in qualified/certified EHRs but also to PHI maintained in any format including paper records. Then, the 2016 Guidance applied the fee limitations indiscriminately without regard to content, usage or recipient. Further, OCR applied some of the fee limitations of paper record collection from the original Privacy Rule to the new requirements, preventing providers from charging fees for pulling the records together and sending them to parties other than the patient and personal representative using them for treatment purposes. *As a result, OCR blurred the distinctions between recipients, usage, and content of the records and did not address the significant difference in the effort required to provide the USCDI via a C-CDA or FHIR API as compared to the at times enormous effort required to provide any data outside of the USCDI, such as images, particularly when data in the designated record sets lies in multiple systems and formats (both electronic and non-electronic).* With multiple EHRs and modes of storage, as referenced above, it can take weeks of work to put together a response to a single patient's designated medical record set for a third party using the records to make a profit or that is otherwise monetizing those records.

B. This expansion has opened the floodgates to access to sensitive patient data under the patient directive by third parties and has the potential to create a major patient privacy issue, exposing private patient data to the public in a mass breach, without any legal liability to the recipient that is receiving this sensitive data legally and without restriction under the patient directive.

The intent of the HITECH Act was clear from its language. It was intended to grant third parties the right to receive an electronic copy of an individual's EHR provided that (1) such an EHR was, in fact, used and maintained by the individual's provider and (2) the individual directed such production. That statutory requirement, without more, would not have been unduly burdensome. However, the regulatory expansion of this third party right -- which did not distinguish between electronic data maintained in a qualified/certified EHR and all other data – greatly expanded the

[3] Pub. L. No. 111-5, 123 Stat. 226 (2009).

burden borne by providers. Moreover, the 2016 Guidance made matters worse by concluding that the patient fee limitations were also available to third parties receiving records pursuant to a patient directive.[4] In an effort to ensure that patients could use apps and patient portals more effectively and without a large price tag to access their electronic data, HHS inadvertently opened the floodgates of third party access to all patient data, regardless of format, and regardless of the purpose for which the data is being accessed, all at little or no cost to the third party.

One unintended consequence of this expansion is the reduction of patient privacy - because it has given third parties that are not HIPAA covered entities or business associates easy, no cost access to troves of patient data that can be used, monetized or resold in any way they choose (because they are not governed by HIPAA), often without patients even having any awareness of the third party's intent or actions. This is now happening at significant and increasing volumes as an ever-expanding group of third parties becomes aware of this potential windfall. These medical records contain sensitive information concerning sexual preferences, including information concerning an individual's LGBT status, sensitive information about women and children and crimes that have been committed against them, information concerning sensitive and personal diseases and medical conditions (hepatitis, AIDs, cancer, obesity), information regarding substance abuse and addiction, and private information including race, social security and financial information, etc. This information can end up in the hands of parties outside healthcare for commercial use and without any privacy requirements under the expanded patient directive. This can increase the likelihood of the next potential privacy breach if non- providers and non-business associates are invited to gather information for commercial use under the patient directive. The elderly in particular are vulnerable to unscrupulous actors that seek to profit from the use of sensitive information.

C. This expansion also has created a new industry intent on regulatory arbitrage – to gather records for their commercial benefit and shift the cost of this record production on to the U.S. healthcare system of providers. This cost shift from commercial parties is costing providers more than $1.52 billion annually and $22 billion in lifetime regulatory cost.

To date, trial attorneys have received almost all of the benefit of this multi-billion dollar cost-shift ($1.52 billion annually[5] and $22 billion in lifetime regulatory cost). Sometimes, these firms indiscriminately submit multiple record requests to disparate health systems for the same records set, because there is no cost to them, thus exponentially increasing costs to the providers and waste of human effort and time.

---

[4] https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/access/index.html

[5] *See* footnote 2, *supra.*

Moreover, it is now clear that things will only get worse. The expansion of the patient directive has also spawned the formation of new companies and industries to capitalize on the patient directive (intended for patient treatment) and place the burden of their start-up costs directly on the providers and the U.S. health system. These industries are making large profits at the cost of increasing the burden on providers. This is increasing healthcare costs and exacerbating the administrative burden on providers as well as detracting time and attention from taking care of patients.

The following is an example of how this is currently occurring in the industry. Third parties, including entities that are not subject to the HIPAA Privacy Rule, such as law firms and data collection companies, have patients sign a form (either paper or electronic) directing wide-ranging production of patient PHI to the third parties at the patient rate. The third party then submits the request to the provider organization, requesting the full designated record set, not simply the USCDI, and requires that the provider give them all records under the Patient Rate or, in some cases, at no cost. This is a form of regulatory arbitrage where individuals are making profits based on the regulations and guidance and placing that burden on the providers and the U.S. health system. Once obtained, the third party may then use the data for any purpose, including selling the data to marketers, pharmaceutical companies, etc., since they are not limited in their use of data by HIPAA. Patients are often not informed about how the third party will use the data, and in many cases the patient is not even gaining access to the data. *The 2016 Guidance effectively created an environment for third parties to access data at no or little cost, place the financial burden of their costs on the providers and the U.S. health system, and then profit off of such access, all while putting patient privacy at risk as described above.* As mentioned, to add insult to injury, providers (which themselves are facing mounting financial pressures) are left to absorb the cost of providing such data to these third parties, effectively allowing third parties to unduly profit from provider absorption of the costs which amount to more than $1.5 billion annually.

Recommendation 1 (A. and B.)

Ciox Health requests that ONC recognize the above-described burden and unintended consequences as a priority area to be addressed by HHS in the next iteration of its Strategy. We understand that ONC is not primarily responsible for the HIPAA Privacy Rule and guidance. Consequently, to address this burden, we recommend that ONC work with OCR and CMS to review the Privacy Rule and OCR FAQs to accomplish the following as soon as possible.

A. Indicate that the Patient Rate applies only to requests provided in response to a patient directive that is truly patient-centered, i.e., those from the patient, and those from the patient's Personal Representative for Health Care Purposes, for purposes of managing the patient's health. The Patient Rate would not apply to any requests for such records to be sent to any party other than the patient or his or her Personal Representative.

AND

B. Address third party access to clarify that only the data included in the USCDI is required to be produced under the Third Party Directive. Access to all other patient data is properly available under a Patient Authorization. This clarification of existing law and regulations acknowledges the difference between (a) the small effort required to provide the USCDI data from a certified EHR via a C-CDA or FHIR API and (b) the sometimes enormous and time consuming effort needed to provide all other patient data to third parties. It would also recognize the intended distinction between patient treatment and other uses of such data.

Together, these changes would relieve the financial burden being placed on providers and help protect patient privacy, while still providing patients with easy, low cost access to the data they most care about when managing their health and wellness.

Recommendation 2

A second area of burden missing from the strategy document relates to interoperability and the data overload it can create for providers. We are encouraged to see the progress the industry has made on exchanging health information, with close to half of ambulatory providers and 90 percent of hospitals sending and receiving data electronically.[6] Such data liquidity is vital to providing more effective and efficient care to patients. However, the current data exchange being undertaken does not take account of what data is necessary to share and when it is necessary to share it. As a result, rather than sharing salient data points with ambulatory providers about patients in their panel, hospitals are inundating providers with C-CDAs that sometimes can be hundreds of pages long. Providers, nurses, and care managers have to dig through mountains of data to find the actionable data points needed to manage the care of their patients. This is further compounded by the inability of EHR systems to incorporate data in patient records in a correct format and location. ONC's most recent data indicates that only 31 percent of ambulatory providers and 53 percent of hospitals can integrate electronically received data into their EHR.[7] This creates a significant burden on providers both in the amount of time they have to spend to read through lengthy C-CDAs and the inherent risk of missing a salient piece of data. The burden caused by data overload was not articulated in ONC's strategy, and we recommend that ONC add this to its next iteration. Further, to address this issue, we recommend that ONC work with the industry to ensure that EHRs can integrate data from the USCDI into their systems, regardless of where the data originates. We also recommend that ONC

[6] 2018 Report to Congress: Annual Update on the Adoption of a Nationwide System for the Electronic Use and Exchange of Health Information. ONC. December 2018. https://www.healthit.gov/sites/default/files/page/2018-12/2018-HITECH-report-to-congress.pdf

[7] *Ibid.*

work with the industry to expand the USCDI over time by incorporating additional high priority data elements that EHR vendors will be required to support.

Conclusion

Ciox Health strongly supports interoperability of data for both patients and providers. Interoperability is crucial to improving patient care and safety and decreasing the cost of care. We firmly believe in a patient's right to access and use their data to improve and manage their own health and the health of those for whom they provide care. We believe that common sense regulations and guidance can correct the above-noted unintended consequences created by existing regulations/guidance that are putting patient privacy at risk and creating a significant burden for providers and their staff, and that ONC should work with OCR to accomplish this as soon as possible. We stand ready to work with ONC to better understand the other burdens and challenges described in this letter and create strategies to address them.

Thank you,

Sincerely,

Donald H. Romano