3 June 2019

Don Rucker, MD
National Coordinator
Office of the National Coordinator for Health Information Technology (ONC)
U.S. Department of Health and Human Services

Re: HHS-ONC-2019-0002-0001 - 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Dr. Rucker,

Thank you for the opportunity to provide input on this proposed rule.

Clinical Informatics, Inc. assists healthcare entities, government agencies, and software developers address challenges in strategy, policy, and innovation. We take an holistic approach when responding to each challenge, including when responding to proposed federal rules.

ONC has done an excellent job of navigating numerous challenges in crafting this proposed rule. We generally support both the intent and the language of the rule in most areas. Herein we focus on a small number of issues we would like ONC to reconsider, two of which ask ONC to coordinate with the Office of Civil Rights (OCR) and the Office of Inspector General (OIG).

We ask ONC to consider making small adjustments in the rule to ensure that:

- the 7 interoperability exceptions do not become the new barriers to interoperability,
- harm of patients is minimized by supporting their transition from having limited or no access to their data, to becoming their own data stewards,
- all data sharing is based upon or makes use of standards, and
- API Users are differentiated into two distinct groups, Third-Party Developers and End Users.

Ensure interoperability exceptions don't become the new path to data blocking

We support the concept that circumstances can be highly variable among the many healthcare environments and what may be easy, obvious, and inexpensive in one environment, may be the direct opposite in another. As such, it is both appropriate and necessary for the final rule to allow for exceptions. However, exceptions could be used to block data sharing if the rules that guide their use are not explicit about what constitutes a valid exception or if the rules are not clearly tied to a well defined and highly publicized enforcement mechanism. The risk of using exceptions to inappropriately block data sharing is true for all of the exceptions, but the exceptions for infeasibility and harm seem most easily abused if not carefully defined, so we focus on them to offer two examples.

In financially troubled health systems and entities, it should not be a valid exception to say that everything is too expensive to implement, even if the local financial limitations make software upgrades difficult to budget. Infeasibility should apply to specific data requests, not to all requests. Conversely, if a data provider can share data in any manner required by this rule, but chooses not to provide data in the specific manner requested by the data requester, the requirements of this rule should be considered satisfied and no exception for infeasibility should be needed. The parties can negotiate a solution or the data requester can transform the data themselves into the format they desire.

As clinicians do what is best for patients to the best of their ability, fear of harm can lead to inadvertent data blocking. There continues to be a perception among some well-meaning clinicians that no data should be shared with patients due to the fear that it might harm patients psychologically or emotionally in the absence of clinical context provided by the clinician. Existing data has refuted this perception, but in the absence of clear guidance in the exception, it could still be used by well-meaning clinicians to block or limit data sharing.

Request
In this context, we ask ONC and OIG to work together to:
(1) provide clear examples about what constitutes a valid exception for a specific patient data request,
(2) provide at least one clear example of what does not constitute a valid exception,
(3) make clear that no exception may be used for a group of patients (whether grouped by institution, clinical practice, clinician, specialty, or any other group of patients),
(4) ensure that enforcement is progressive but swiftly applied in response to blocking complaints received, and
(5) publicly post all actions taken in order to educate and promote awareness.

Support patients during this time of transition

It is wonderful that the 21st Century Cures legislation has shifted our national conversation from paternalism (*whether* to share data with patients) to collaboration (*how* to share their data with them). This change in mindset is critically important if we want to better engage patients in their care and move our entire health system toward a more cost-effective one, promoting better health at lower cost.

Every national transition carries a risk of harming the people we want to help. As we begin this transition, very few patients have previously evaluated any Third-Party Developers ("Developers") for the risks of sharing data with them. There will be no common knowledge about either the Developers themselves or what methods are effective to evaluate them. Star ratings in an app ecosystem will provide no useful information in this regard. If we allow this void to persist without adding appropriate patient supports, many patients are likely to be harmed by sharing their data with Developers who plan to sell their information in order to provide the product for free, build a large customer base, and make a healthy profit. There is nothing wrong with a healthy profit. It is a requirement for a business to remain in business. What is problematic is that there are no rules to enable patients to fully evaluate Developers so that a free market can occur.

Perhaps some population of patients have no aversion to their data being sold. Those patients may not have any increased risk without a framework of rules. Maybe they will make the same choices regardless of available information. However, government has an obligation to manage the common spaces where we meet and engage in commerce, which means there is an obligation to ensure that those who *do* care about having their data sold should be provided a mechanism to learn that information.

Developers must be transparent about how a patient's data is managed, stored, and transmitted.

ONC should set a minimum bar for Developers that mimics the nutrition labels we have on food today. As a consumer, you can choose to ignore the information. No one is required to read it. However, those who wish to know the information before making a purchase can make an informed choice.

Below we consider this labeling in two ways, the rules themselves and how the rules are enforced.

Request

We ask ONC to use the CARIN Code of Conduct (the "Code"), or a similar set of privacy components, to define the labeling of third-party software that wants to act as a proxy for the patient requesting Electronic Health Information. This request focuses not on using this Code specifically, but on the types of information that the Code describes. This Code describes privacy considerations that Developers should describe for patients who are considering a Developer's product. If ONC prefers to develop its own code, that could also ensure that patients have the transparency needed to make an informed choice. This request does not require any Developer to agree to the Code, merely to complete a standardized form (like a nutrition label) that states how the Developer manages patient data.

For example, if ONC chose to utilize a modified version of the Code, a completed form from developer XYZ might look like this:

Share data with whom you designate	yes
Share data with marketers without explicit consent	no
Share data with partners without explicit consent	yes
Comply with COPPA	yes
Provide advance notice of policy changes	no
Limit health data requests to only what you request	no
Securely dispose of your information at your request	no
Protect your health information	yes
Maintain data provenance, when provided	no

Imagine that developer ABC has responded as follows:

Share data with whom you designate	yes
Share data with marketers without explicit consent	no
Share data with partners without explicit consent	no
Comply with COPPA	yes
Provide advance notice of policy changes	yes
Limit health data requests to only what you request	yes
Securely dispose of your information at your request	yes
Protect your health information	yes
Maintain data provenance, when provided	yes

If you were a consumer, which product would you choose?
Isn't it clear that the mere ability to know about the Developer's choices will force all products to better support patient needs **and** allow patients to make more informed choices?

For this transparency to occur, there must be a lever. A Developer whose product least benefits the patient will want this information to be hidden. As such, some Developers, perhaps a large cohort, will not voluntarily share this information. While there may be many ways to ensure that all Developers

share this information, enabling HIPAA defined Covered Entities (CEs) to be the lever is probably the lowest cost and most effective option to ensure that all Developers, regardless of country of origin, will be required to post this information. ONC should work with OIG and OCR in this effort. OCR should adjust its prior guidance to require CEs to withhold data from Developers who fail to post this information about their product. No transparency → no patient data → no customers → no profit. This simple lever will ensure that all reputable Developers will share this information in order to get the data that will enable them to get customers and remain financially viable. It also ensures that Developers who would willingly support their patients by providing this information are not penalized for sharing information that their competitors are hiding. It supports a level playing field.

This move toward enforcing transparency will not in any way harm the free market or limit choices made by patients, but will make knowledge available to support a free market. If there are concerns that patients should be allowed to choose from among any and all Developers, then this rule could sunset after 5 years so that community knowledge can be built first. This would stage our national transition to support patients now and allow for all comers once the transition is farther along and the likelihood of injuring patients is much reduced. Let us not move the pendulum from share no data with anyone to share all data with everyone. We can be more measured in our approach to move data sharing forward in a way that supports each patient's ability to choose and also allows them to make informed choices.

Lastly, a standard set of privacy component descriptions would also serve a voluntary certification process. Certifying entities could arise to test and evaluate whether the products actually adhere to the Code components in the way the Developer says they do. Reputable Developers may choose to pay these entities to gain a seal which reassures patients and would have value and meaning, even if these privacy components sunsetted and were no longer a requirement.

All data should be in a standard format

If we want data to be interoperable, its semantic meaning must be preserved. To maintain semantic meaning, the data must be in a recognizable format. If we allow any data to be transmitted in a non-standard format, that data will effectively be useless, and potentially dangerous due to misinterpretation by less informed (or more brazen) software developers. Standards are not a barrier to data sharing, they are its foundation, a necessary condition.

Request

ONC should require existing data standards to be used by all parts of this rule. When shared data is unstructured, it should use an existing standard for unstructured data. When data is structured, it should use the most applicable standard for structured data. When there is no applicable standard for the structured data, it should be transmitted using an existing unstructured data standard. ONC should work with standards organizations and developers to rapidly define a header format, or select one that exists, that will allow for accurate interpretation of the structured data by including this header at the beginning of the unstructured data file.

The concept of an API User needs to be split to reflect the very different members of that group

Both in what we have discussed thus far and in other parts of the proposed rule, it is clear that Developers and patients have very different roles to play, very different rights and responsibilities. Having only a term that combines them into a common group makes it too easy to confuse those roles, rights and responsibilities. As such, two new terms are needed. The existing term may have value, so it

need not be eliminated, though its current usage could be replaced by mentioning both new terms where both apply and the single new term where only Developer or patient is intended.

Request
ONC should create a Third-Party Developer term to reference the subgroup of API Users who provide software that is directed to patients and their legal proxies. ONC should also create an End User term to identify those API Users who are patients or their legal proxies.

Additional thoughts

Messaging about some comments submitted for this proposed rule are becoming public. In this letter, we want to clearly support ONC moving forward with this rule by addressing one of those public messages. No one wants their power or money diminished. The 21st Century Cures legislation (at least as applies in this paragraph) is to partially remediate the market perturbation created by the Meaningful Use (MU) program which gave Electronic Health Record (EHR) vendors a power advantage in the usual customer relationship. MU made purchase of software that didn't meet user needs a legal requirement, rather than allowing the marketplace to decide when a product actually met user needs. This perturbation of market forces requires ongoing legislative countermeasures in an attempt to require the products to meet a minimum level of utility, interoperability in this case. These are the types of things that users might demand in an elastic market but cannot effectively do with a mandated product that is costly and difficult to replace and where an oligopoly exists. A government requirement that EHR vendors must meet these conditions as a cost to play in this market-altered space is both reasonable and necessary, similar to the conditions leading to the existing EHR certification programs.

We also wanted to offer a few comments on the Request for Information about patient matching. First, ONC is correct in asserting that no technology can resolve poor data. This is a key component of why no single identifier is sufficient to uniquely and consistently identify an individual. If any one identifier is entered incorrectly or fraudulently presented, it detracts from identifying a patient. As such, the continued cries for a "unique" identifier are unhelpful. Imagine a patient arriving in an emergency department (ED) insisting they be treated but only sharing "I am 5654-234-4990." Maybe they remembered the number wrong or one of the nines was heard as a five. No ED would treat a competent patient without at least their name and birth date. We always want and need corroborating data, so the concept of a unique identifier is fanciful. Second, ONC is correct in suggesting that additional insights about patient matching are needed and additional data elements may be useful. The California Medicaid program began adding mother's first name to their records as part of an identification process in the 1990s that markedly improved matching rates above using social security number. ONC should consider (a) creating a laundry list of identifiers currently in use, (b) assemble a list of personal identifiers not currently in use (e.g., height or eye color), and (c) work with a research partner to assess which combination of identifiers is most likely to accurately identify an individual. Once this information is known, ONC could then add these identifiers to the USCDI so that when they are collected, they are collected and shared in a prescribed way. In addition, this research should identify primary identifiers that have the highest likelihood of indicating a match, and secondary identifiers to use when the primary identifiers are absent. There may be a ratio of 2 secondary identifiers being needed for each primary identifier that is missing, or perhaps the ratio is different, but the process used, the algorithm, should take into account the lower likelihood of accuracy with the secondary identifiers and weight them accordingly.

As we make this very important national shift to sharing data, we must keep our focus on the goal: better health at lower cost. We should ensure that we do not succumb to the idea that one "must" break a few eggs. While we can never eliminate all risks, we can anticipate several risks of this transition. Once recognized, we should not sit by and let those risks become actual harm. For the benefit of all Americans, we ask you to carefully consider the few adjustments we request ONC make to this rule.

Thank you.

Larry Ozeran
President
Clinical Informatics, Inc.
http://clinicalinformatics.com/
lozeran@clinicalinformatics.com
(530) 650-8245

CLINICAL
INFORMATICS