Massachusetts Health Data Consortium

Congressional RFI: 21st Century Cures Act and Cures 2.0

This document was submitted by the Massachusetts Health Data Consortium (MHDC) and its Data Governance Collaborative (DGC) on July 30, 2024 in response to the 21st Century Cures Act and Cures 2.0 RFI posted by Congress on June 6, 2024 and found here:

https://files.constantcontact.com/e7a90be4701/543bdffd-4cf7-48ef-9a14-3c413a8a9f4c.pdf

About MHDC

Founded in 1978, MHDC, a not-for-profit corporation, convenes the Massachusetts's health information community in advancing multi-stakeholder health data collaborations. MHDC's members include payers, providers, industry associations, state and federal agencies, technology and services companies, and consumers. The Consortium is the oldest organization of its kind in the country.

MHDC provides a variety of services to its members including educational and networking opportunities, analytics services on both the administrative and clinical side (Spotlight), and data governance and standardization efforts for both clinical and administrative data (the Data Governance Collaborative/DGC and the New England Healthcare Exchange Network, respectively).

About DGC

The DGC is a collaboration between payer and provider organizations convened to discuss, design, and implement data sharing and interoperability among payers, providers, patients/members, and other interested parties who need health data. It is a one stop interoperability resource. The DGC primarily focuses on three areas:

1. Collaboration: Development of common understanding of and specifications for data standards, exchange mechanisms, and what it means to participate in the modern health IT ecosystem
2. Education: helping members understand their regulatory obligations, the data and exchange standards they're expected to use, and modern technology and related processes
3. Innovation: Identification and development of projects and services needed to make modern health data practices and exchange a reality

Approach to RFI

MHDC and its Data Governance Collaborative focused on questions 2 and 3 in the RFI:

2. What elements might be missing that are essential for further progress?
3. What additional reforms, support mechanisms, or incentives are needed to enhance or improve the effectiveness of the steps already taken, including any structural reform to agencies, offices, or programs involved?

We have gathered our feedback and suggestions into categories, presented below.

In addition, we have called out a few areas that may or may not be outside of the scope of Cures 2.0 legislation but that we feel require Congressional action and thus are worthy of discussion in an overarching healthcare modernization bill. We leave it to Congress to decide if they fit in with plans for this legislation or could be considered in other future legislation.

General Suggestions

This section will provide general suggestions that cut across different components and goals of the Cures Act.

Technical and Financial Assistance

Many data, health IT, and interoperability provisions of laws and regulations are essential for moving the goals and programs of the 21st Century Cures Act and any follow up legislation forward, but many of them can also be prohibitively expensive for smaller healthcare or other related organizations from the standpoint of time, resources, and staffing.

Including funding for both financial assistance and support for technical assistance would help these organizations keep pace with health data and health IT requirements they need to operate in the modern world. It is not helpful to have increased functionality available in a certified EHR or a payer health IT module if the prospective users cannot afford to use it either because of the added expense or the added burden of implementation, integration with existing processes and workflows, and new training.

Centers of Excellence

Many data, health IT, and interoperability provisions of laws and regulations are essential for moving the goals and programs of the 21st Century Cures Act and any follow up legislation forward, but many of the individuals using them are not experts in these areas and, even if they can afford specialists, the available work force of experts is likely not sufficient to meet all of the needs of the industry, at least not during phases when everyone is trying to plan, implement, test, and operationalize projects at the same time.

Even if larger organizations have onsite health IT, data scientists, data analysts, and other relevant staff, these individuals likely are not experts on the specific requirements or elements of new programs that stem from new laws and regulations. They may need help using or understanding the related tools and technology. Smaller organizations are less likely to have any staff or related expertise at all.

We believe creating Centers of Excellence that can provide guidance, advice, support, education, etc. on specific key areas would be extremely helpful to the industry at large. Perhaps they could also provide discounted implementation help for certain qualified organizations. Some suggested areas include:

- Artificial intelligence
- Privacy
- Security
- Health Equity and SDOH
- Health IT Infrastructure (identity, consent, provenance, etc.)

There are almost certainly other functional areas that would also benefit from this type of set up.

We note that regional assistance centers were used during the initial implementation period for EHR software. This type of model could be resurrected and revised to meet these current and future needs, especially if discounted implementation help that would be more difficult to provide from a single centralized location is one of the available programs. Even if regional centers are adopted, it may still make sense to centralize some informational/educational oriented components to reduce duplication of efforts across different regions.

Alignment of Plan Types

It is increasingly difficult to manage different workflows, processes, and requirements for different types of plans. Pushing alignment across not just various government plans but also commercial plans would be extremely helpful in many areas including:

- Interoperability requirements
- Prior authorization requirements

- Price transparency requirements
- Reporting requirements

In some cases (such as for the No Surprises Act) requirements already extend across all or most plan types, but many data, interoperability, and health IT requirements imposed by law and subsequent regulations are only applicable to government plans (one or more of Medicare, Medicaid, CHIP, exchange plans, etc.) and sometimes there are inconsistencies and differences between the various government plans. This makes it difficult or impossible to have a single standard implementation across all plans supported by a payer or for a provider with patients spanning different types of payer coverage.

The single biggest complaint we hear from payer and particularly provider members of MHDC (both in the DGC and outside of it) is the need to reduce the number of variations of data specifications and exchange methods for various use cases. Ideally, they would be able use a single, well understood data standard and data exchange mechanism that encompasses all necessary use cases between exchange partners, but barring that be able to do so for each use case independently. Having different requirements for different plan types makes this significantly more difficult.

Consistency Across Federal and State Exchanges

As a corollary to the last topic, there are times when specific requirements are placed on fully qualified exchange plans under the Affordable Care Act where the requirements apply to all such plans and other times when they only apply to plans managed on the federal exchange at healthcare.gov and not to those managed directly by states (such as mahealthconnector.org) even though all of these plans are supposedly filling the same role in the healthcare ecosystem.

This is confusing and problematic, and it seems like a loophole that should be closed.

Development and Alignment of Standards and Standard Components

Different agencies and even different groups within the same agency pick and choose from among multiple available standards for things like:

- APIs and other transaction mechanisms
- Code sets and value sets
- Implementation Guides and specifications
- Quality measures, rules, and guidelines (clinical or other)

They do not always make the same decisions, and sometimes their decisions are incompatible with each other. It would be helpful to include mechanisms to require better communication and coordination around various types of standards and standard components across these groups.

All of the participants in our Data Governance Collaborative find this burdensome, overly complex, and expensive, but our payers seem to be particularly affected by these differences.

Standard Requirements and Advancement

Participants in our Data Governance Collaborative strongly recommend a policy whereby standards are not set in legislation or regulation, but that these documents point to external definitions that can referenced by multiple rules (in support of our last topic) and updated outside of the legislative and regulatory processes as needed.

ONC does have the optional SVAP process allowing optional use of newer versions of some standards so long as they are backwards-compatible with the mandated version, but the required versions are all outlined in specific rules that can be misaligned between different rules, be difficult to locate within incredibly long rules (recent CMS and ONC rules have often been between 800-1100 pages long), and difficult to maintain as they are repeated often throughout each rule when they apply to multiple components of the same rule.

We recommend requiring maintaining a single external source of truth for required versions of standards

located at a specific and well documented location online that everything else can reference.

Increased Opportunities for Standardized Interoperability

We believe that there are many additional areas, use cases, workflows, and projects that would benefit from increased interoperability. We believe HHS (and other agencies as appropriate) should be authorized and encouraged to actively seek out and explore these opportunities. Related activities could include new interoperability rules, new certifications, funding for pilot projects, participation in workgroups and industry projects looking into new areas of interoperability, and more.

For example, increased interoperability around various types of specialty care would be extremely helpful. As follow up to a public deep dive our Data Governance Collaborative ran on the data and interoperability needs in physical therapy, we started working with a physical therapist to further delve into the specific needs of this constituency and what it would take to support their data and health IT needs in a consistent, standards-based way. We had some similar discussions around eye care after our deep dive covering it. So far nothing concrete has come from these projects, but we believe that there are significant specific data and interoperability needs of these and other communities within healthcare that should be explored and (hopefully) implemented in the future.

In addition, there are many patient-facing tasks that could only benefit from additional data standardization and interoperability requirements. One such example is plan shopping/choosing a new health plan. Having standardized processes and APIs that can be used to gather data that third party apps could use to help patients with this task (either on its own or as part of a suite of patient services) would be extremely helpful. These could be used to help compare specific exchange-based plans or specific Medicare Advantage plans or, ideally, specific commercial plans offered by an employer using the particular needs of the patient or group of patients (spouse/family) trying to select a new plan. In a perfect world, a patient could even compare the plans their employer offers with exchange plans or compare plans from the employers of two spouses to help them decide which one to choose.

Information Blocking

This section will provide suggestions and comments specific to information blocking and the oversight of related activities.

ONC Ability to Provide Clear Guidance on Specific Circumstances

ONC is currently hampered by an inability to provide specific guidance or responses regarding whether specific circumstances would be considered information blocking.

ONC has requested greater authority in this area in each of the last several congressional budgets without success. This authority is necessary for the industry as a whole to have clear expectations around what behavior is acceptable vs considered information blocking

As things currently stand without this authority, much of the guidance and advice given by ONC amount to “it depends” or “sometimes” or other equally frustrating responses that do not provide clarity to the organizations trying to determine their obligations under law. This is incredibly frustrating and often leaves organizations unclear on their actual obligations around information blocking even if they have the best of intentions around compliance.

Clearly Defined Actors

While the statutes and regulations define three actors/roles under which information blocking applies, ONC has made it clear that these roles do not match up 1-1 with organization types. For example, payers are not explicitly named but may qualify as an information blocking actor as a provider, a certified health IT vendor, or an HIE depending on the circumstances (https://www.healthit.gov/faq/are-health-plans-or-other-payers-subject-information-blocking-regulation). Other organization types may find themselves in a similar place.

This is confusing and makes it difficult to determine whether or when a particular organization is, in fact,

subject to the information blocking rules. A useful update to the information blocking law and subsequent regulations would be clearly defining whether or not specific types of organizations are subject to information blocking without relying on the role they're playing at the time of the request for information.

Should Have Known Standard for All

Current statute has different definitions for information blocking for providers vs other actors: certified health IT vendors and HIEs have a "should have known" standard for being held liable for information blocking while providers have an actual "did know" standard.

While we do not wish to place additional burden on providers, the "did know" standard is too high a bar, one that can easily be avoided by a simple attestation by a key individual regardless of whether it defies logic that they did not know (i.e. that they clearly should have known).

Participants in our Data Governance Collaborative believe 'should have known" is a reasonable standard to apply to anyone subject to information blocking and the minimum needed for effectiveness.

Provider Disincentives Tied to Other HHS Activities

As currently written, provider disincentives for information blocking must be tied to other programs they're using within HHS. This means that providers that do not qualify for these programs have no penalty/disincentive for information blocking.

So far, a limited number of CMS programs have been identified as meeting the requirements for disincentive eligibility. The way these programs are structured, the available disincentives may only be applied once per year, and often there is a delay in notification/applicability.

This means that there is no incentive to fix information blocking issues until the next year's program starts, or, conversely, that notice of non-compliance may come at such a time where the provider cannot fix issues in time for the next year and will automatically be in violation for an extra program year (provided someone complains in the new program year).

Further, this means that providers will only be notified of their first information blocking infraction since this is the only one that comes with a disincentive. A better system would notify providers of every infraction so they can fix all of the different ways they might be information blocking within the course of a single year and be more likely to be in conformance in subsequent years rather than get dinged once per year until all of their issues are discovered and fixed.

Participants in our Data Governance Collaborative believe the way these incentives are currently applied are very limited and are not equitable across the ecosystem of providers that may, in fact, be guilty of information blocking since many of them may not belong to a program with available disincentives.

Further, even if the current disincentive system remains intact, the DGC strongly believes that providers should be notified of all adjudicated information blocking claims that result in a finding of guilty whether or not they result in official disincentives. This reduces the likelihood of entering into a years long chain of fixing one issue per annual disincentive notice as described above and also gives providers that may not qualify for an actual disincentive the chance to fix their issues anyway even if they are not going to be penalized for failing to do so.

Data Integration

This section will provide suggestions and comments concerning integration of data from various sources.

Incorporating Data from Exchange Partners

Current rules require various data exchanges between payers, providers, patients, and other relevant parties. However, other than integration into future data exchange in some cases, there are limited requirements around directly using this data or making it an integrated part of the relevant patient records.

Such integration should be required (with relevant provenance attached) so it can be used in future care decisions, as information shared with others in future exchanges mandated by CMS and ONC, and for other

useful purposes alongside any relevant directly generated patient data.

Pharmacy and Other Specialty Data

Behind the scenes certain types of medical care have very different processes, health IT, data standards, and the like. However, from a patient perspective it's all health care and there's no logical reason why this care should be separate or unavailable when the same data is available for other services that use different back end processing.

At a minimum, all patient-facing data and exchange requirements should include all of the data patients would consider relevant, even if behind the scenes the processing happens in different ways.

For example, pharmacy data uses different standards, workflows, and exchange mechanisms than other types of medical data. Patients can get their patient records via FHIR APIs including information about the medications they take and the status of their prior authorizations excepting medication prior authorizations. Even though the underlying mechanisms for processing PA requests is different, the resulting status and information should be required to be included in patient visible prior authorization information regardless of how the patient requests it (Patient Access API or portal or other mechanism)

Further, the current landscape does not consider data exchange between payers and PBMs (for example). Participants in our Data Governance Collaborative strongly believe that PBMs should be required to use the same standards payers and providers are expected to use for medication data and related data exchange to make it easier to integrate data from PBMs into payer systems and vice versa. Similarly, for other types of specialty care that may be carved out on the payer side or use different IT on the provider side, any relevant IT systems should be required to use the same data and exchange standards as payers and providers do for that type of care.

Further, all relevant health IT should be encouraged or required to certify against the same relevant standards regardless of whether the IT system is being used by providers, payers, PBMs, or another type of organization being used as part of the healthcare ecosystem. If relevant standards do not exist to support such certifications, they should be developed.

Medical and Wellness Devices

Currently, even if use is prescribed by a clinician solely to collect data (such as a blood glucose monitor or blood pressure cuff), there is limited integration of medical device and wellness device data into patient health records. Participants in our Data Governance Collaborative believe any such data directly provided to clinicians at their request should be integrated into the patient's medical records.

As this data originates outside of the healthcare ecosystem, consent is likely required. Provided the patient is told or provided information about how it will be used, we presume the act of deliberately providing the data to a clinician is sufficient consent, but requiring explicit patient consent would be fine. Assuming this consent is either implicitly or explicitly given, the data should be part of the patient record and available across the healthcare ecosystem in accordance with normal data/data sharing rules.

Originally, we planned to propose this integration be automatic, but participants in our Data Governance Collaborative were concerned about potential patient matching issues and believe a basic review and approval from a clinician or relevant staff should occur first to ensure the correct data is being attributed to the correct patient. However, to prevent indefinite delays, they believe a specific time limit should be placed on this review and, if not explicitly accepted or rejected within this allowed period, the data should be automatically accepted into the patient record. They also felt industry input was needed to determine the appropriate timeframe to wait prior to automatic integration and declined to suggest one at this time.

Data supplied by the patient without clinician input/request should not be subject to this requirement but may be integrated into the patient record once reviewed by their clinician if the clinician wishes it.

Data Privacy

This section will provide suggestions and comments concerning data privacy.

Non-Profit Loophole

One of the big concerns around the use of third party applications, medical devices, and other digital technologies is data privacy. This is overseen in two different ways: HIPAA for covered entities and their business associates and the FTC Health Data Breach Notification rule (and similar authorities) for others.

However, the FTC has no authority over non-profit organizations, just for-profit businesses. Thus, there is a loophole in the current privacy landscape for applications, devices, and other technologies from non-profits when their offerings are not under the auspices of HIPAA.

There needs to be some type of similar oversight for these options, whether through an expansion of the FTC authority or otherwise. We do not have enough understanding of the various levers of the federal government to suggest exactly how this oversight should work or which agency should be responsible for it if the FTC authority cannot or should not be expanded to encompass it.

What Constitutes Health Data/Health Information

The definition of PHI officially used in HIPAA is not necessarily expansive enough for patient protection in the current data landscape and other definitions are used in other laws and regulations across various agencies.

Identifiable health-related data can be found via geolocation data, retail purchases, electronic calendars and address books, and other applications and related data stores we don't necessarily consider directly health related.

The FTC just addressed this to some extent in their recent update to the Health Data Breach rule, but we feel strongly that a more comprehensive and consistent mechanism for addressing this is warranted.

Medical, Wellness, and Home Health Devices

Medical and wellness devices generate a lot of patient data. This data is often held under the control of the medical device manufacturing company, often without patient knowledge. Home health devices that come directly from providers should also be part of this discussion if their data is owned/stored/controlled by the manufacturer rather than the provider organization overseeing use of the devices.

For example, manufacturers of CPAP devices often collect and store significant data about the breathing and sleeping habits of patients using their devices and resell that data for marketing purposes, share it with payers to be used in coverage decisions, and more (see https://www.propublica.org/article/your-medical-devices-are-not-keeping-your-health-data-to-themselves).

Consents, if collected at all, are buried deep in initial contracts and similar documents and are not obvious to affected patients.

Participants in our Data Governance Collaborative believe better disclosure and consent around collection, storage, exchange, and use of this type of data should be required. In particular:

- Explicit, clear consent in a separate consent form should be required
- Separate consent should be required for each purpose/type of data use
- Separate consent should be required for each new data exchange partner including both providers and payers (even if they ordered the device or are paying for the device; payers should only get financial information and not patient usage data without consent)
- A mechanism for reviewing and revoking consents should be available

Properly Removing Expiring Data

Properly removing data that has an expiration date is part of good data hygiene and can help limit the impact of

any privacy violations that do occur by limiting the amount of data actually captured in a breach.

Participants in our Data Governance Collaborative would like to see mechanisms put in place to ensure data with an expiration date is deleted (or perhaps archived for a time in a protected area before deletion) from certified health IT.

HIPAA Administrative Simplification

This section will provide suggestions and comments concerning HIPAA Administrative Simplification requirements and their impact on health IT projects and data interoperability.

Required Transactions

The HIPAA Administrative Simplification rules require that certain electronic transactions use specific X12 EDI formats and mechanisms.

There are newer and, in some cases, more efficient ways to complete some of these transactions leveraging FHIR and other mechanisms in some use cases/workflows.

The current HIPAA requirements place limitations on newer, innovative projects that wish to use FHIR for things like referrals unless they are willing to do onerous translations between FHIR and X12 solely to comply or they fall under limited exceptions such as:

- Approval for an exception via a very onerous, time-limited process that poses a significant risk to organizations that use it (since they may have to stop using it after devoting time and resources to building out the process using an alternate mechanism)
- Enforcement discretion offering some relief for prior authorization transactions complying with recent CMS rules

Rather than enforcement discretion, our Data Governance Collaborative believes it would be better to change the underlying law to make requirements more flexible as the enforcement discretion could, in theory, also go away at any time.

Further, more rapid and less onerous mechanisms to allow for use of newer technologies such as FHIR should be integrated into HIPAA Administrative Simplification rules. Our staff know of several proposed FHIR projects that were considered by various groups but not launched because they would have violated HIPAA transaction requirements without an exception or some other mechanism for using FHIR instead of X12 for referrals or other transactions subject to the rule.

Legislation that makes these types of changes possible, exceptions faster and less onerous, and experimentation less risky would be greatly beneficial to the industry as a whole.

Redundancy Requirements

MHDC believes that organizations should be required to maintain redundant connections for required X12 EDI transactions so that the impact of outages such as the one caused by the Change Healthcare cyberattack cause significantly less disruption to the industry.

Some specific things we believe should be required include:

- Payers required to maintain multiple connections; exclusivity with a single clearinghouse should not be allowed
- EHRs required to readily re-route to a secondary EDI vendor if their primary vendor is down (may require some re-enrollment or pre-enrollment for some payers; as much pre-enrollment should be done as allowed)
- Clearinghouses required to attest they maintain multiple pathway options to connect to each payer and support re-routing capabilities for redirecting traffic along those pathways in the event of an outage

Patient Access

This section will provide suggestions and comments concerning various aspects of patient access to both data and care.

Consent

MHDC firmly believes patients have the right to control their own data, who sees it (as much as possible), and how it is used. Current electronic consent practices are not very granular and do not give patients much control over what data is covered and how it is used.

Things like independent second opinions are very difficult in a world without granular consents, and patients may be reluctant to share certain types of particularly sensitive data without restricting its use (and each patient may have a different definition of what they consider sensitive or wish to hold more closely than other data).

Paper consent forms still provide options to limit consent to specific types of data, specific files, specific encounters, specific reports, specific time frames, etc. Until electronic consent mechanisms allow the same level of granularity and control, patients will continue to prefer paper consent forms to maintain the level of control they're used to having and want to maintain over their medical data.

While HIPAA permits certain data use and exchange without patient consent, and information blocking and federal API rules may mandate some of that data to be exchanged without requiring consent, patients should be asked to consent as often as possible to engender trust in the system and to give them control over who sees their data. In particular, patients should be able to designate data they consider sensitive as such and exchanging it with anyone should require explicit consent.

Even though demographic data is important for health equity and reporting reasons, data such as race, ethnicity, religion, sexual orientation, gender identity and similar should be allowed to be marked as sensitive with the rules outlined above to maintain trust with marginalized communities. For example, we have heard transgendered individuals discuss how they've shared their gender identity with providers they trust and ended up with other providers they did not choose to share it with have access anyway via various data sharing that happened behind the scenes without consent. They considered this a form of being outed; it made them distrustful of healthcare writ large.

In addition, MHDC and participants in our Data Governance Collaborative believe most FHIR data exchanges should require patients to opt in. At the current time, some are opt in and some opt out. In particular, the current CMS Provider Access API included in the CMS-0057 Interoperability and Prior Authorization rule finalized earlier this year and set to go into effect on January 1, 2027 currently allows patients to opt out. We believe it should require patients to opt in instead (we realize the current model is likely set in stone at this point and, to be transparent, we provided this same feedback during the public comment period for the proposed rule and it was not acted upon then). We propose that future interoperability laws require patients to opt in whenever their data is being exchanged for treatment-related activities. Business operations, such as exchange of clinical or patient data needed to calculate quality measures, should be allowed without consent so long as specific restrictions patients have placed on the exchange of particular data elements they consider sensitive are respected.

Finally, our Data Governance Collaborative believes patients should have a role in defining whether a treatment relationship exists with a specific provider. As part of a consent system, it would be nice if patients could either review providers claiming to have a treatment relationship for purposes of the Provider Access API and either approve or reject them or explicitly list those providers they wish to designated as having a treatment relationship with them. In addition, patients should be able to view and revoke existing patient relationships. The current Provider Access API certification does not address the treatment relationship requirement at all; addressing it this way would put the power of consent in the hands of patients where we feel it belongs.

Transparency and Traceability

MHDC firmly believes patients have the right to control their own data, who sees it (as much as possible), and

how it is used.

To support this, participants at our Data Governance Collaborative believe patients should have a view of all organizations, applications, and other entities with active consents and a view of all actual data exchanges performed using their data whether or not consent is required.

Further, patients should know where any specific data originated and where it was modified regardless of who they obtain it from (full provenance of data throughout its lifecycle).

Finally, there should be standardized APIs or other mechanisms developed that support development of tooling to support this level of transparency and traceability of data.

We note the treatment relationship designation discussed in the consent topic just above this likely should be part of these transparency and traceability APIs.

Right to Forget/Right to Correct

While the majority of healthcare providers act in good faith and capture relevant, useful data about their patients, periodically things go wrong. There may be visits with known false conclusions, incorrect data captured, where providers make snap judgements, or otherwise generate data that is not correct and could be detrimental to a patient if it persists in the system.

As data exchange is becoming more common and widespread, bad data can proliferate and follow patients across their healthcare journey. Patients should have the ability and right to either have certain records siphoned off from the system as “deleted” or to have them corrected when errors are found. Prior to HIPAA this right to forget was available to patients in many jurisdictions (using the paper records of the time). Bringing it back can only improve the quality of data available in the system and give additional control over their data back to patients, something MHDC feels strongly about.

A solution for dealing with how to get coverage/payment for visits where the data has been “deleted” should be developed that does not require re-introducing the bad data into the patient’s records, especially since payers are generally mandated to include any clinical data they have in Patient Access, Provider Access, and Payer=>Payer APIs.

Accessibility

Accessibility, be it accessibility for disabled patients, for patients with low English proficiency, patients with poor health literacy, or patients in other circumstances with addressable accessibility issues, should be required when possible and promoted/encouraged when it can’t be required.

Certified health IT supporting patient access should be required to meet basic standards of accessibility for certification in each of the areas above as well as any other areas identified by Congress, HHS, or other relevant agencies.

Mobile apps from state and federal governments are newly required to be accessible to the disabled, as are apps from commercial organizations covered by the ADA, but there are many holes and oversight is not centralized.

Any actions that could be included to promote or require accessibility of third party apps used for healthcare (in all of its variations) should be pursued.

Payer and Provider Access

This section will provide suggestions and comments concerning payer and provider access to data and tooling.

Accessibility

Accessibility is often something that’s considered and provided for the public or for customers or for users but employees are people with disabilities and other issues/circumstances people experience.

It is reasonable to expect English proficiency and good health literacy from employees in healthcare and

health-adjacent settings, but accessibility for non-English speakers would be a bonus.

Health IT should be required to meet basic standards of disability-related accessibility for professional users in order to be certified.

Anything that can be done to promote or require disability-related accessibility in other health IT including mobile applications used in the professional setting should be pursued.

Mandates on Health IT Users in Addition to Certified Health IT Developers

While there are many organizations that adopt new technology because it's beneficial and will help accomplish their business goals, many others are already overburdened and under resourced and only adopt those things they are required to use in order to meet mandates or ensure payments for their services.

At the current time, while there are some incentives within various CMS payment rules, the vast majority of the mandates around certified health IT are around what certified health IT modules must support and make available to their users, not around requiring use of those features. ONC specifically and HHS more generally often talk as if once a feature is mandated for inclusion in certified health IT it is automatically in widespread use by the providers using that health IT (until the recent HTI-2 proposed rule, all certified health IT was for provider use), but providers still need to turn on and pay for specific features they wish to use. In many cases, these features don't make the cut unless included by default without extra cost and implementation time or needed to meet one of those incentives from CMS (see topic below for more on this).

In order to ensure widespread access, use of certified Health IT by providers should be mandated in some way. If this is not possible, significantly more incentives are needed to encourage additional functionality to be enabled. As we are unfamiliar with all of the available levers to do this, we will refrain from suggesting exactly how this should be done.

That said, we do have one suggestion in this area: to adopt the financial incentives from our general suggestions above and tie them specifically to implementation of specific features of certified health IT deemed particularly important such as FHIR API support (see topic below for more on this).

Any such programs should be designed to encourage use of certified health IT at all organizations with available certified health IT (including payers and public health departments once the ONC HTI-2 rule is finalized), although the current landscape means providers are generally more in need of this type of assistance/push to adopt.

Cost of Certified Health IT

While we do not begrudge certified health IT developers a healthy profit for their work, participants in our Data Governance Collaborative and other providers we've heard speak on this topic at industry events feel like EHRs are nickel and diming them to death. Every new feature requires a new fee, and turning on FHIR APIs is no exception.

We have heard many providers indicate they have chosen not to enable FHIR functionality because it's not mandated and it costs extra money they cannot afford or would rather spend directly on patient care.

One suggestion in this area is to adopt the financial incentives from our general suggestions above and tie them specifically to implementation of FHIR APIs so they can only be used to pay for these fees or fees related to implementation, configuration, or other related services.

Similar funds should also be available to small payers for IT (once the ONC HTI-2 rule is finalized and certified health IT is available to them) and other smaller organizations that may have difficulty affording or prioritizing spending money on certified health IT that would improve their data quality, interoperability, reporting, or other important functions.

Another suggestion is to require or encourage "all inclusive" models. However, these likely have the disadvantage of raising the bar of entry since the baseline price would, necessarily, increase for this type of model.

Regardless of the specific option/mechanism, some means of addressing this issue is essential to ensure that

the majority of providers are able to take advantage of modern health IT, improved data standards and data quality, and increased interoperability between payers, providers, patients, and others.

Payer and Provider Tooling

This section will provide suggestions and comments on recommended tooling required to help users of health IT perform the tasks they need to accomplish

Tooling for Reviews

Participants in our Data Governance Collaborative believe a tool for managing reviews should be developed and required for both payer and provider IT. The tool should allow individual users to request all items awaiting their review, all items by type, all items with a deadline in the next N days, all items with a deadline in the next K hours, and other functionality as deemed appropriate/useful.

One use for this tool would be reviewing the incoming data to approve integration into local systems per the topics above under Data Integration, and it originally came up in that context in our discussions. However, our participants believe a more general tool might be helpful, one that could also be used to manage things like “sign off on patient discharge” or “sign off on order for Y” or other tasks that might require clinician or staff review on a regular basis.

In an ideal world, this tool would include standardized API access to allow for app development outside of clinical systems, such as the development of mobile applications to manage these approvals.

Prior Authorization Tooling

Although the new HTI-2 proposed rule includes API certifications for prior authorization, it does not appear to include any requirements for workflow support around prior authorization.

Some features provider tooling should support include:

- Provider delegation of prior authorization requests to a work queue upon popups via order-sign and order-select CDS Hooks
- The ability to assign prior authorizations in the queue to specific staff members to follow from creation to disposition
- The ability to search for specific prior authorizations by assigned staff, patient, provider, type of service, status, and date range
- The ability to find requests that do not require a prior authorization
- The ability to check the status of a prior authorization request based on the unique ID returned by the CRD API
- Notifications when responses are received from the payer, sorted by response type (approved, denied, pended) so next actions can be taken if needed (a secondary sort on denial reasons may also be useful)
- The ability to pass an authorization number to revenue systems for claims processing for locally provided services
- The ability to track expiration date or remaining amount for locally provided services
- The ability to send an authorization number to an external provider for related services
- The ability to send email, text, or in-system notifications based on preference choices of each user

Provenance Tooling

Participants in our Data Governance Collaborative believe tooling for tracing the full provenance/history of specific data including its original source, each organization that stored the data then passed it on unchanged,

each transport mechanism used to move the data, and each time it was modified or edited in any way should be available both to users of certified health IT and to patients accessing data via certified APIs (see Transparency and Traceability section above for more on the patient access recommendations).

Business Processes Around Technology

While we called out several specific workflow tools above (both in this section and under the Patient Access section) we believe that explicit consideration of the business processes around specific technology should be required. Certifying APIs is a great step, one that is necessary, but it is not sufficient if the business and operational workflows incorporate those APIs into the actual activities of the employees needing the data being exchanged.

Considering the operational workflow support needed for this should be part of any API-related certification offered by ONC/HHS. APIs are not used in a vacuum, but rather to supply the data needed to feed tools that do something useful within a specific context. Without the step of considering how APIs could be used and requiring some standardized basic tooling to support this within useful workflows, the APIs themselves have significantly less value.

Certification

This section will provide suggestions and comments concerning both voluntary and required certifications.

Certification of USCDI+

ONC has been releasing a variety of data sets in conjunction with federal partners called USCDI+. Each of these data sets is focused on a specific area (at the current time, data sets exist in at least draft state for maternal health, public health, behavioral health, quality, and cancer). These data sets are positioned as sets of data needed to properly conduct healthcare in each of these areas and ONC has generally noted they are intended as floors for data support in the same way that USCDI is the floor for healthcare data generally.

However, none of these data sets have widespread adoption. One issue is that, unlike support for the more general USCDI, there are no certification programs to indicate whether any specific health IT modules or tooling support any or all of these data sets.

Participants in our Data Governance Collaborative have been finding it progressively more difficult to understand the intent and scope of some of these data sets as currently presented and in understanding how they are likely to be used within healthcare operations focused on their supposed areas of coverage. They feel certification programs would be an excellent step toward promoting clearer communication around the expectations of each data set as well as their adoption in any type of consistent, usable way.

Certification of Tooling

Any workflow tool, patient access tool, or new API adopted in a Cures 2.0 law should have a corresponding certification program for each of the payer, provider, or other organization expected to use the tool as standalone health IT or within other certified health IT platforms (such as EHRs). A partial list of certifications that might be appropriate if all of the suggestions within this comment are adopted include:

- Review/Approval workflow tooling
- Prior authorization provider workflow tooling
- Provenance tooling
- Patient consent/transparency API (provider)
- Patient consent/transparency API (payer, including treatment relationship designations)
- Review/Approval API
- User Accessibility certification

- Patient Accessibility certification
- Removal of expired data certification

Some of these could, perhaps, be collected into category-based certifications or ingested into larger existing certifications (for example, removal of expired data likely could be part of a more general certification program).

Certification for Payer and Other Health IT

ONC has been discussing the possibility of certifying payer health IT for several years now for both AI and prior authorization (there may be other areas under consideration as well, but these are the only ones that have been discussed publicly as far as we know).

The HTI-2 proposed rule was released while we were in the process of writing this comment and it includes the very first payer certification programs covering components of the various CMS payer APIs including the Patient Access API, Provider Directory API, Provider Access API (both payer/server and provider/client), Payer=>Payer API, and Prior Authorization API (both payer and provider). Only the provider APIs are mandated and the payer APIs do not seem to include effective dates at this time so it's not clear when they might become available for optional use.

We applaud these baby steps into the payer health IT world, but suggest that certification in additional areas would be helpful. Participants in our Data Governance Collaborative have expressly called out pharmacy-related interoperability between payers and PBMs as a particular pain point; they would love to see certification of health IT on both sides of the equation mandating use of various pharmacy standards (NCPDP, FHIR, and others as appropriate) so that payers can use the same systems for communications with providers already using these standards and PBMs which are not.

ONC should be asked to look for other areas and technology where wider certification programs make sense and explore/implement them. We believe all relevant health IT should be encouraged or required to certify against the same relevant standards regardless of whether the IT system is being used by providers, payers, PBMs, or another type of organization being used as part of the healthcare ecosystem. If relevant standards do not exist to support such certifications, they should be developed.

Certification of APIs or Tools from CMS or other Agencies

We will discuss this topic in more detail below under the coordination topic, but additional coordination is needed for certifications based on APIs or other tools developed/designed/mandated outside of ONC such as the CMS APIs included in the HTI-2 proposed rule.

The certification programs in that rule exhibit something of a chicken-and-egg issue where ONC notes they are not including features or versions or items that are not explicitly required by the related CMS rules, but those rules were finalized before those features/versions/items existed - and in at least most cases the CMS rule allows for their use by virtue of their adoption by ONC either directly or in the SVAP optional version advancement process.

Some type of directive to develop features and their related certifications in tandem so they match would be helpful. We realize that might make life more difficult or cause the rule of one agency or the other to be delayed solely because the other agency has other priorities that are taking precedence at that given moment, but if it leads to significantly better alignment across the related rules we respectfully suggest it's worth the wait.

Inter and Intra Agency Coordination

This section will provide suggestions and comments concerning coordination of across different agencies or different organizations within HHS (such as ONC and CMS).

USCDI+

The USCDI+ program has been generally positioned as a series of joint efforts between ONC and other federal agencies or organizations within HHS to develop minimum necessary data sets for interoperability around

specific types of healthcare.

In general discussions about the program, ONC has noted they expect their partner agencies to use USCDI+ data sets within their regulations when those regulations pertain to areas with an existing USCDI+ data set. However, at the current time, this does not appear to be happening.

Right now, there are just lists of data sets without status (i.e. whether they are in draft, constitute a version 1 released set, etc.) and without any indication of use or intent. As noted above, these are no certifications against any of these data sets to provide assurances that health IT support any or all of them (or at least those that may have progressed beyond draft status, if any have).

It is possible that the USCDI+ program has not progressed to the point where actions by partner organizations should be expected, but the lack of communication around any of this – status, intended use, versioning, and more – makes it difficult to understand how much time, energy, and resources should be spent on trying to understand, work with, and plan for these data sets.

Additional clarity in these areas as well as a clear and consistent design paradigm for these data sets used consistently across all of them would go a long way toward helping health IT developers and users understand and potentially use these data sets. Prior to intended use, the development of certification programs (likely including some form of testing mechanisms) and other support/workflow items typically developed for new types of health IT and health data standards should be required.

Incompatible Rules

As noted in several places throughout this comment, better alignment across related rules from different agencies or, sometimes even the same agency (two different related CMS rules, for example), is necessary to make the regulatory health IT process run more smoothly. Whether it's using different definitions for the same terminology, requiring different versions of the US Core at the same time, starting provider-side Provider Access API certification a year after support for the API is required, requiring prior authorization supporting data be available to Patient Access/Provider Access/Payer=>Payer APIs in FHIR formats but proposing requirements to use X12 275 for attachments (based on a letter sent to HHS in 2016; the attachments final rule was delayed after significant public call to support FHIR), it is more common than not that two regulations that overlap in some way include at least some incompatible or not easily compatible requirements.

Participants in our Data Governance Collaborative, particularly the payers affected by these types of issues in recent interoperability rules, find managing these issues incredibly difficult, expensive, time consuming, and frustrating.

Any actions Congress can take to improve coordination between agencies would be greatly helpful (this can also be an issue between two related rules from the same agency, such as the aforementioned CMS prior authorization and attachment rules). The most common interagency issues seem to occur between CMS and ONC around interoperability, HHS and FTC around data privacy, and ONC and OMB around race and ethnicity definitions.

Certification Issues

ONC's HTI-2 proposed rule includes several certifications for CMS APIs. The certification requirements for some of these APIs impose specific requirements when several options are allowed by CMS (which is totally fine) but also do not always include all of the requirements imposed by CMS for those APIs. For example, the Provider Access API requires that a provider show they have treatment relationship with a patient before being granted access to that patient's data. While we recommended adopting specific rules in our comment to the related rule, CMS chose not to specify a particular mechanism for determining how or for what rules to use. Rather than come up with a set of rules required for certification (which would have been in keeping with other decisions made in these certification programs), ONC ignores the requirement entirely.

Both providers and payers can certify against the ONC requirements and never develop any mechanism for determining if a treatment relationship exists. There isn't even a need to supply something like an attestation as part of the API call or similar. This means both parties can pass the ONC certification without meeting the actual requirements imposed by CMS. The missing requirement is an important privacy protection for patients

and, should certified health IT developers solely use the ONC certification requirements to implement their APIs based on an expectation that certifications must impose all necessary features of the API, patient privacy could be seriously violated as providers with no reason to hold the patient's data would be able to acquire it.

Telehealth

This section will provide suggestions and comments around the permanent adoption of telehealth

Making Telehealth Support Permanent

Access to various types of telehealth and remote monitoring services has been a godsend to many patients. While it has been particularly advantageous for a variety of disadvantaged communities (the disabled, folks without sick leave at their jobs, folks in healthcare deserts, etc.) it is a useful option for everyone.

Avenues such as audio-only telehealth have been particularly helpful to disabled patients and should remain available to increase their access to care. Requiring retention of these care modalities is important for all patients, but especially for addressing health equity issues. In particular:

- Ongoing support should be required for all plan and payer types
- Ongoing support for these modalities (including audio only telehealth) should be encouraged at provider organizations (perhaps tied to health equity quality measures or other programs)