Federation of American Hospitals®
Charles N. Kahn III
President and CEO

June 3, 2019

Don Rucker, MD
National Coordinator
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
330 C Street SW, Floor 7
Washington, DC 20201

Re: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program; Proposed Rule (RIN 0955-AA01)

Dear Dr. Rucker:

The Federation of American Hospitals (FAH) appreciates the opportunity to comment on the Office of the National Coordinator for Health Information Technology's (ONC) *Proposed Rule: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* published on March 4, 2019 (Proposed Rule). The FAH is the national representative of more than 1,000 investor-owned or managed community hospitals and health systems throughout the United States. Our members include teaching and non-teaching hospitals as well as short-stay, rehabilitation, psychiatric, long-term acute care, psychiatric, and cancer hospitals across urban and rural America, and they provide a wide range of acute, post-acute, and ambulatory services.

The FAH continues to believe in the potential of health information technology (health IT) to improve the quality and efficiency of care provided to patients, reduce provider burden, and advance population health management and breakthroughs in health care research. As we have noted in previous comment letters, the *Health Information Technology for Economic and Clinical Health* (HITECH) *Act* catalyzed broad adoption of electronic health records (EHRs), but the use of such technology has not yet achieved the quality and efficiency goals desired by stakeholders across the health care sector. The inability of EHRs to both exchange and use information is a significant barrier to achieving these goals. Congress recognized this barrier in enacting numerous policies in the *21st Century Cures Act* (Cures Act). The FAH appreciates

ONC's commitment to advancing interoperability and offers the below comments and recommendations to guide these efforts. Given the significant interaction between the ONC Proposed Rule and the Proposed Rule from the Centers for Medicare & Medicaid Services (CMS), the FAH comments on the CMS Proposed Rule are provided herein as Attachment A.

III.B.1. Removal of Randomized Surveillance Requirements

The current regulatory requirements for Authorized Certification Bodies (ONC-ACBs) regarding in-the-field surveillance and maintenance of certification of health IT[1] are only being implemented for reactive (*e.g.*, complaint-based) surveillance. ONC has exercised enforcement discretion regarding randomized in-the-field surveillance of certified health IT modules by the ONC-ACBs since September 2017. In the Proposed Rule, ONC proposes to remove the requirement for ONC-ACBs to conduct randomized surveillance for a minimum of two percent of certified health IT products per year, instead making such surveillance voluntary. Requirements for reactive surveillance would continue unchanged, including the option to use an in-the-field approach.

As the FAH previously commented in response to ONC's EHR Reporting Program Request for Information (RFI), the lack of randomized, in-the-field surveillance leaves a significant gap in the ability to determine real-word conformance to certification testing and maintenance of certification, as well as to improve health IT capabilities related to security, interoperability, and usability.[2] In those comments, the FAH urged ONC, at a minimum, to look to the in-the-field, randomized surveillance regulatory requirements as a starting point from which to build the EHR Reporting Program. The FAH also encouraged ONC to look beyond the current requirements to develop a more robust, collaborative surveillance and improvement model using an independent testing/accreditation body that would examine the use of health IT in the field.[3]

While the FAH does not oppose revision of the current, partially enforced ONC-ACB surveillance requirements, we recommend that the intrinsic value of in-the-field surveillance be considered during the development and deployment of real-world health IT testing and as ONC's EHR Reporting Program evolves. More information regarding the above-mentioned collaborative surveillance model, as well as the FAH's comments and recommendations regarding ONC's proposals for real-world testing of certified HIT can be found below in Section VI – Real-World Testing.

[1] 42 CFR 170.556.
[2] FAH response to the Request for Information Regarding the *21st Century Cures Act* EHR Reporting Program (October 17, 2018).
[3] This independent body could be a testing organization, such as the ONC-ACBs, or an accreditation organization, such as those currently used by the CMS to determine compliance with CMS regulations.

IV. Modifications to the 2015 Edition Certification Criteria

Edition Designation and Clarity of Final Criteria

ONC proposes an extensive set of changes to the Health IT Certification Program's 2015 Edition. Besides the addition, removal, revision, and updating of multiple criteria, ONC makes several proposals that affect the standards and implementation specifications for health IT certification. The FAH recognizes the imperative for ONC's Health IT Certification Program to keep pace with changes in health care delivery and health IT while advancing interoperability and is generally supportive of ONC's efforts to maintain the relevance and currency of the program. **Given the extensive changes proposed in the rule, however, the FAH believes that a new Edition designation is necessary, particularly given the identical or very similar descriptors of some old and new criteria (*e.g.*, data segmentation for privacy).** At a minimum, ONC should clearly identify the most recently adopted criteria and present them together in a form and manner that is intrinsically intuitive to users based on input from developers, providers, and end-users.

Promoting Interoperability Program (PIP) Alignment

The FAH appreciates the recent, significant collaboration between ONC and CMS to move toward a shared vision of interoperable health IT in support of federal health care programs and the patients they serve. The PIP components of several CMS payment systems require hospitals and health care professionals to utilize 2015 Edition CEHRT, and multiple CMS performance measures link to 2015 Edition certification criteria.

Further progress towards interoperability while minimizing provider burden depends upon continued ONC and CMS collaboration. As such, **the FAH strongly urges that all finalized changes to the 2015 Edition certification criteria be carefully aligned with CMS initiatives. Particular attention should be given to eliminating all the PIP uses of certification criteria removed by ONC and ensuring that the retained criteria are sufficient for robust support of the PIPs.** Building upon its experience with CMS, ONC should explore opportunities to collaborate with other state and federal agencies to limit overlapping reporting requirements for providers.

United States Core Data for Interoperability (USCDI) Standard

ONC proposes that the Common Clinical Data Set (CCDS) definition be removed and replaced with the USCDI standard, adding several new data classes for which interoperability would be required (*e.g.*, pediatric vital signs). Once finalized, ONC would implement an open, annual-cycle process for expanding the USCDI as described elsewhere and designed to be collaborative, predictable, and transparent.[4] **The FAH supports the proposed transition from CCDS to USCDI and the draft annual process for USCDI expansion.**

[4] Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process, available at https://www.healthit.gov/sites/default/files/draft-uscdi.pdf

Electronic Health Information (EHI) Export Certification Criterion

ONC proposes to update the 2015 Edition by removing the current "data export" criterion and replacing it with a new "EHI export" criterion. Health IT certified to the new criterion would be required to support timely full migration of all of the EHI produced or electronically managed by a developer's IT for two use cases: 1) a single patient who requests their health data, and 2) a provider who requests health data for any subset or the entire database of their patients when transitioning or migrating to a new IT system. The following features would be required of the export files: 1) be electronic and in a computable format, and 2) be exported with information about the file's format, including structure and syntax, that is available by a publicly accessible hyperlink. Developers would be given flexibility to determine their products' export standards.

The FAH has long supported patients' rights to access their health care information under the *Health Insurance Portability and Accountability Act of 1996* and its implementing regulations (collectively, HIPAA) and recognizes the importance of usability and user-centered design as health IT performance metrics. Conceptually, the FAH agrees with ONC's goal of facile electronic health data exportation but has reservations about several operational details as proposed. First, we are unclear about what ONC intends by requiring that data be exported in a computable format. The FAH agrees that the exported data should be in a digital format but notes that some data for export may not be computational in nature (*e.g.*, a PDF document). **The FAH urges ONC to clarify the intended meaning of computable.**

Second, while the FAH supports consistency in how the EHI export criterion is applied to single patient and patient population data requests, we note that the end-users of data exported for the two use cases are quite different in their actual data needs, health IT literacy, and treatment under the law. Usable data exported to a single patient for use in their own care differs substantially from the data required by a provider about their patient population to facilitate full migration during an IT system transition. The overarching challenge of EHI export is tailoring the exported data to be sufficient to meet the user's needs but not excessive; large and poorly structured data dumps are not useful to patients or providers and could produce the same undesirable results (even though wholly unintended) as other forms of information blocking.

The FAH recommends that ONC allow for variations in functionality appropriate to the two use cases when assessing health IT modules submitted for certification to the EHI export criterion. For example, under HIPAA, a single patient user is entitled to access to his designated record set, not all of which may be available in an electronic format (as discussed in more detail in Section VII – Information Blocking). **As such, the EHI export should be limited to the EHI collected and retained by the certified EHR. For IT system transitions, the FAH supports the proposal to require vendors to provide a data map, and notes that the identification or creation of a consensus standard for vendors may also be needed.**

Third, ONC proposes that developers and providers would implement the EHI data export criterion within 24 months of the effective date of ONC's subsequent final rule. The FAH does not believe that the allotted time will be sufficient for developers and providers to fulfill their respective roles as required by this criterion. Developer module creation and testing will consume much if not all of the 24-month period. Hospitals and health systems, clinicians, and

other providers will need time to safely and effectively implement these changes, including staff education and training on how to assist patients with formulating their data requests and, as data providers, to respond to patient requests. **The FAH recommends that ONC extend the implementation timeline, allowing two years for developer rollout and an additional year for health care provider implementation.**

Finally, the FAH believes that harmonization of regulations and metrics across health care delivery system components whenever feasible is a characteristic of high-performing systems. **Therefore, the FAH strongly recommends that ONC continue to collaborate closely with OCR and CMS to ensure that patient data access requirements are in line with statutory and regulatory requirements under HIPAA and other federal and state laws and synchronized with Medicare's PIP initiatives and pay-for-performance programs.**

Standardized Application Program Interface (API) for Patient and Population Services Certification Criterion

ONC proposes to remove the "application access – data category request" criterion, replacing it with the new "standardized API for patient and population services" criterion. The new criterion would support API-enabled services involving data from either a single or multiple patient(s) and would require the use of Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) standards. ONC proposes to adopt FHIR Release 2 as the standard for the new API criterion, since nearly 90 percent of hospitals and 60 percent of clinicians are served already by developers with a FHIR Release 2 API.[5] However, ONC further notes the publication of FHIR Release 4 in January 2019, a version that contains highly desirable improvements (*e.g.*, batch exports for patient population data); ONC believes that FHIR Release 4 will become the next *de facto* industry standard. ONC, therefore, offers three alternatives to the proposed adoption of FHIR Release 2 as a sole standard for the new API criterion: 1) adopting Release 4 as a single standard in place of Release 2; 2) allowing developers to choose certifying to either Release 2 or Release 3; and, 3) allowing developers to choose certifying to either Release 2 or Release 4.

The FAH appreciates ONC's efforts to strike a balance between the maturity and the capabilities of the available Releases when choosing a FHIR standard. Meeting any new API standard will entail reconfiguration of numerous interfaces, necessitating large investments of time and money. The FAH agrees with ONC that FHIR Release 4 is likely to emerge quickly as the next industry standard, and we note that only Release 4 can manage population level data, an activity essential to value-based care delivery. In addition, Release 4 is the first release of FHIR being developed with backward compatibility in mind for high-priority FHIR resources, making it a stronger foundation for future development. Older releases of FHIR are not backward compatible and would not be well-positioned to keep up with the USCDI, which will evolve on an ongoing basis. As such, the FAH believes that time and monetary resources would be most prudently invested by concentrating on deploying the single, best available FHIR standard. **The FAH recommends that ONC adopt FHIR Release 4 as the sole standard for the API certification criterion.** By skipping multiple, incremental upgrades, moving directly to FHIR

[5] ONC indicates having derived these results from data published by developers on the Certified Health IT Products List (CHPL) as of mid-September 2018.

Release 4 will most efficiently bring API developers, technology suppliers, health care providers, and users most quickly to a single, sophisticated, shared API platform.

Relatedly, ONC proposes a 24-month API FHIR standard implementation period, beginning with the effective date of a subsequent final ONC rule. This timeline is insufficient for health IT developers and API Technology Suppliers to complete and rollout their products and for data providers, such as hospitals and health systems, to implement those products, including designing and delivering staff education and training programs.

The FAH strongly recommends that ONC extend the API standard implementation timeline for at least a year to allow all participants to reach the levels of functionality required by their distinct roles in EHI exchange. An extended timeline also would allow for testing strategies to mitigate our members' concerns about unintended privacy consequences that could arise when patients unknowingly allow redirection of their EHI to others through third-party applications that may not be HIPAA-compliant (as discussed in more detail in Section VII – Information Blocking). **The FAH also urges CMS to maintain the reporting period for PIP at 90 days at least until the transition to FHIR Release 4 has ended.**

VI. Conditions and Maintenance of Certification for the Health IT Certification Program

Section 4002 of the *Cures Act* provides for ONC to establish Conditions and Maintenance of Certification requirements for its Health IT Certification Program. ONC proposes seven Conditions plus Maintenance requirements for health IT developers and their certified modules related to Information Blocking, Assurances, Communications, APIs, Real-World Testing, Attestations, and EHR Reporting Criteria Submission. The first six are proposed for implementation in ONC's subsequent final rule, while the EHR Reporting Criteria Submission is deferred to future rulemaking.

Assurances: Record and Information Retention

For Maintenance of Certification under the Assurances Condition, ONC proposes that health IT developers be required to retain records and information necessary to demonstrate ongoing compliance with ONC's Health IT Certification Program. Specifically, ONC calls for a ten-year record retention period starting from the date a developer's health IT is first certified under the Program. A three-year retention period would be required for health IT for which all certification criteria have been removed from the Code of Federal Regulations (CFR), starting from the effective date of criteria removal from the CFR. **The FAH supports retention of information via the Certified Health IT Products List (CHPL) and further recommends retention for a period of seven years for health IT for which all certification criteria have been removed from the CFR.** The seven-year retention window for removed health IT would be consistent with the audit look-back period for providers, and we note that our members often retrieve documentation from the CHPL during the audit process.

Communications: Developer "Gag Clause" Removal

ONC further proposes a Communications Condition of Certification that would not allow health IT developers to restrict or prohibit communication about their products' features or

performance in the areas of usability, interoperability, and security, or about the developers' business practices (*e.g.*, contractual "gag clause"). With very limited exceptions, users could not be prohibited from exchanging information about their experiences with a developer's modules, including purposes for and methods by which users have deployed the modules. **The FAH strongly supports the proposed Communications Condition of Certification.** Unrestricted sharing of real-world experiences among users of a developer's modules is critically important in the areas of patient safety and security; multiple instances of patient harm triggered by poor usability have been reported.[6] Furthermore, transformation to value-based health care delivery would be accelerated by enhancing the ability of health IT users to exchange information about best practices and successful strategies.

ONC proposes a two-part, 24-month timeline for Maintenance of Communications certification to begin with the effective date of ONC's subsequent final rule. Within the first six months, each developer would be required to notify all customers that any communication or contract/agreement provision violating the Condition would no longer be enforced by the developer, and the developer must provide repeat notification annually until the offending provision is removed. Within 24 months, all developers would be required to have amended all contracts/agreements to be compliant with the Communication Condition. **The Federation fully supports the complete removal of "gag clauses" but has reservations about the feasibility of ONC's proposed timeline. The FAH supports the six-month period for initial customer notifications by developers**. However, the 24-month period available for all developers and all their customers to have completed execution of new or amended contracts may be too short, particularly if a developer does not provide the draft contract to customers until late in the allotted time period. **The FAH recommends that developers be required to submit compliant contracts to customers within 18 months, allowing customers at least a six-month period to review, finalize, and execute the contract.**

Application Programming Interfaces and Third-Party Applications

The ONC Proposed Rule proposes policies to govern requests from API Users (*e.g.*, third-party applications) to access certified API technology. Currently, many API Data Providers (organizations, such as health care providers, that deploy, or contract with the API Technology Supplier to deploy, the API technology) rely on their API Technology Suppliers (health IT developers that create certified API technology) to perform a review of such requests. The Conditions and Maintenance of Certification proposals in the Proposed Rule, however, would limit the ability of API Technology Suppliers and API Data Providers to keep malicious applications from connecting to the API. For example, the API Technology Supplier can, but is not required to, verify the API User's request to access the API, but this authentication is only at the API User entity level, not for each application the entity seeks to connect. Additionally, as drafted, it appears the ONC Proposed Rule absolves API Technology Suppliers that do not have an authentication process from responsibility for connecting to poorly designed or malicious applications. If finalized, these proposals will cause API Technology Suppliers to scale back their current review processes and may cause smaller API Technology Suppliers to abandon their review processes entirely due to the expected volume of API User requests and the limited time

[6] Jessica L. Howe et al., *Electronic Health Record Usability Issues and Potential Contribution to Patient Harm*, Journal of the American Medical Association 319, no. 12: 1276-78 (2018).

in which to perform the verification. This limited verification process is particularly troubling to API Data Providers because, as currently drafted, the ONC Proposed Rule provides them a limited role in this process. While the FAH supports ONC's proposal to give API Data Providers sole authority over who accesses their APIs, such authority has little meaning when the Proposed Rule would not permit them – and most do not have the resources – to verify the security of API Users' applications.

The FAH also has concerns about the proposal to permit third-party applications persistent access to an API via an authorization token that would last for three-months. This proposal raises privacy and security concerns, and the FAH instead recommends requiring reauthentication each time information is sought via the API. Reauthentication at each use is in line with industry standards for accessing other applications containing sensitive information, such as banking or credit card applications, and would not be unduly burdensome on the consumer.

Related to the ONC proposals are policies in the CMS Proposed Rule to require all health plans impacted by the rule to implement, test, and monitor an openly-published API accessible to third-party applications and developers. As part of this proposal, CMS seeks feedback on whether current privacy and security standards, including those under HIPAA, are sufficient to ensure the protection and security of a patient's health information.

The lack of a robust vetting process for third-party applications in the ONC and CMS proposed rules is troubling. The FAH has long supported patients' rights to access their health care information under HIPAA. Health care providers are familiar with the HIPAA Rules and believe they provide important protections for both patients and providers regarding the exchange of protected health information (PHI). Most third-party applications, however, are not governed by the HIPAA security and privacy requirements. FAH members are very concerned that these applications could expose their EHRs to malware, hacking, and data mining. Hospitals must be empowered to protect their systems from unproven and potentially harmful applications and, as such, should not be considered "information blocking" for forgoing relationships with questionable applications.

In addition to security concerns, the FAH cautions ONC and CMS against allowing these unvetted, non-HIPAA-covered, third-party applications fairly open access to patient digital health data without patients fully understanding how those applications might use that data and the implications of that usage. The FAH agrees that it is an individual's prerogative to specify where and to whom to send their designated record set. The FAH does not agree, however, that individuals understand how the information they are sharing will be used and monetized. Most people routinely do not read the entire "terms of use" agreement on every application or website and often mistakenly believe their data is more private or secure than it really is. Recent consumer data privacy events highlight the gap between how companies are using data versus how their customers believe their data is being used. For example, millions of individuals were surprised and angry to learn how Facebook was using and selling their data, while other consumers were not even aware that all their financial information is funneled through three to four credit bureaus, two of which experienced major breaches in the last few years.

Digital data is the currency of the modern technology ecosystem and marketplace, and there are fortunes to be made in mining and monetizing personal digital health data. As such, the rules and processes that govern and protect digital health data must be sensitive to the reality that not all covered entities, business associates, and third parties are created equal. Particularly regarding entities that fall outside of the HIPAA requirements, it is imperative that patients, their families, providers, and consumers can trust that these applications – and the data both sent to and received from them – are secure, private, and clinically sound.

The FAH believes it is possible to support innovation in the marketplace while ensuring the security, privacy, and clinical efficacy of third-party applications through both education and an industry-backed vetting process. In response to the FY19 IPPS Proposed Rule, the FAH urged ONC, CMS, the Office for Civil Rights (OCR), and the Federal Trade Commission (FTC) to undertake a joint campaign to educate patients about the differences between HIPAA and non-HIPAA-covered entities, and how those differences may affect the ways in which their data is used, stored, and shared with others.

Education alone, however, is not enough. Nor is an attestation-only requirement for applications. **An industry-backed process to independently vet third-party applications is needed to ensure they are: a) meeting all relevant security standards; b) using data appropriately and in line with consumer expectations; and c) clinically sound (for those applications that offer medical advice). The vetting process should be at the application level, not just at the entity level; the results of such vetting process should be made public in the form of an application "safe list"; and health care providers and API vendors should be able to refuse to connect to non-vetted applications without running afoul of the information blocking requirements.**

Security

In order to "pass" the vetting process, an application must meet the most current security standards.

Privacy/Data Usage

The vetting should also examine applications' data usage as compared to the more stringent HIPAA requirements and then publicly report those findings for consumers in an easy-to-understand format, such as a simple comparison chart. The FAH also recommends the assignment of an easy-to-understand letter grade (*e.g.*, A, B, C, etc.) to each application based on its data usage, with an "A" grade signaling HIPAA-level protections. The chart and the letter grade would appear to consumers prior to downloading the application or authorizing it to access their health information. The FAH believes this process would enhance consumers' control over their designated record set by enabling them to make fully-informed decisions about where to send that data.

Clinical Soundness

Applications that contain a clinical component would undergo additional vetting to ensure they are clinically sound. The vision for the future includes health care providers pulling information from third-party applications used by their patients and then using

that information to make treatment decisions. That vision is only possible if health care providers – and their patients – can trust the integrity of that information.

Publicly Reported "Safe List"
The vetting organization should publicly report the third-party applications that "pass" vetting for security (and clinical soundness, if relevant) as "safe" for vendors and health care providers to connect to their APIs.

Information Blocking Exception
The FAH strongly believes that all applications seeking to connect to a health care providers' APIs must undergo this vetting process and that providers and API vendors that refuse to connect to non-vetted applications should not be considered "information blocking."

The vetting and public reporting process detailed above will go a long way towards ensuring trust while removing the burden of vetting from consumers, health care providers (API Data Providers), and API Technology Suppliers. The FAH also believes the process has parallels to the "best in class" discussions in the ONC and CMS Patient Matching RFIs. Those RFIs recognize the significant patient safety and patient and provider trust concerns with the current patient matching tools and seek feedback on whether identifying and requiring the use of "best in class" tools would improve accuracy and, by extension, trust. A similar "best in class" thought process can be applied to the vetting of third-party applications, with the "safe list" representing the "best in class" applications.

Real-World Testing

ONC proposes to require developers with certified health IT interoperability- or data exchange-focused modules to test the technology in the setting in which it would be utilized. Under the proposed requirements, these developers would need to annually submit and make public their prospective real-world testing plans and their retrospective real-world testing results.

The FAH has long-supported real-world testing and appreciates ONC's proposals to require vendors to perform such testing. The Proposed Rule, however, does not detail how such testing would work, and thus FAH members are unable to provide specific comments on how it would impact the operations of their hospitals and health systems, including potential IT system and workflow disruptions. **Given these concerns, the FAH strongly urges ONC to be mindful of the burdens this testing may place on health care providers in terms of time and costs and take all necessary steps to minimize such burdens. One way in which ONC can limit burden is by ensuring that health care provider participation in the real-world testing program (and any future EHR Reporting Program surveillance, as discussed below) is *voluntary*, with appropriate incentives to encourage participation.** Such incentives could include: a bonus under the PIPs for hospitals; and a Quality Payment Program (QPP) bonus and/or credit for activities in the Promoting Interoperability or Improvement Activities performance categories for clinicians and groups.

As part of the real-world testing requirements, **the FAH urges ONC to clarify that health IT developers are obligated to correct any deficiencies found during testing as part of their obligations under the Conditions and Maintenance of Certification**. Under the proposed "assurances,"[7] health IT developers "must provide an assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes."[8] If the certified capabilities cannot perform their intended purpose(s) in their intended environment, then the health IT developer has provided a false assurance and is responsible for correcting the deficiency – for all its customers – in order to remain compliant with the Conditions and Maintenance of Certification and the Information Blocking requirements.

The FAH also supports ONC's proposal to require that health IT vendors publicly report the results of their real-world testing. **As part of that reporting, ONC should require health IT developers to be specific about the deficiencies found during testing and the corrective actions the developers took to address those deficiencies.** As health care providers may utilize the same – or similar – technology, public reporting of deficiencies and corrective actions will raise awareness among providers of potential issues within their own health IT systems. This is especially true for deficiencies affecting safety and/or security, which should be publicly reported immediately and for which vendors should bear immediate responsibility to both notify their customers and correct across their health IT products.

In addition to the proposals discussed above, the FAH believes that the implementation of a more robust post-acquisition/post-implementation surveillance program is necessary to truly improve the functioning and use of certified health IT. The current regulatory requirements for ONC-ACBs regarding in-the-field surveillance and maintenance of certification of health IT[9] are only being implemented for reactive (*e.g.*, complaint-based) surveillance. And, in the Proposed Rule, ONC proposes to remove the requirement for ONC-ACBs to conduct randomized surveillance for a minimum of two percent of certified health IT products per year, instead making such surveillance voluntary.

As the FAH previously commented in response to ONC's EHR Reporting Program RFI, the lack of randomized, in-the-field surveillance leaves a significant gap in the ability to determine real-word conformance to certification testing and maintenance of certification, as well as to improve health IT capabilities related to security, interoperability, and usability. **In those comments, the FAH urged ONC, at a minimum, to look to the in-the-field, randomized surveillance regulatory requirements as a starting point from which to build the EHR Reporting Program. The FAH also encouraged ONC to look beyond the current requirements to develop a more robust, collaborative surveillance and improvement model.** Specifically, this model should involve an independent testing/accreditation body that would examine the use of health IT in the field and provide feedback to both health IT vendors and the health care providers who utilize those products.[10]

---

[7] 42 CFR 170.402 (proposed).
[8] 84 Fed. Reg. at 7466.
[9] 42 CFR 170.556.
[10] This independent body could be a testing organization, such as the ONC-ACBs, or an accreditation organization, such as those currently used by the CMS to determine compliance with CMS regulations.

EHR Reporting Criteria Submission

As discussed above, the FAH provided comments in response to ONC's EHR Reporting Program RFI. More information regarding the above-mentioned collaborative surveillance model, as well as the FAH's comments and recommendations regarding ONC's proposals for real-world testing of certified HIT can be found above in Section VI – Real-World Testing and in the FAH's EHR Reporting Program RFI comment letter.

VII. Information Blocking

As noted in previous comments and elsewhere in this letter, the FAH supports the goals of the *21st Century Cures Act* (Cures Act) to further interoperability by ensuring the appropriate movement of clinical data among health care providers and other stakeholders and ensuring patients have access to their data as delineated in HIPAA and relevant state laws.

After passage of the HITECH Act, which accelerated the adoption of EHR systems among hospitals and clinicians, Congress became concerned that some entities were interfering with the exchange of information in ways that prevented the health care system from realizing the goals of an interoperable health system. To ensure that information that can be or should be exchanged under HIPAA and other relevant federal and state laws is indeed being shared, Section 4004 of the *Cures Act* added section 3022 of the Public Health Services Act (42 USC 300jj-52, the "information blocking provision"), which defines and prohibits information blocking.

The FAH supports the goals behind the information blocking provision and the proposed implementing regulations. As health care providers, FAH members have experienced difficultly accessing and integrating clinical information into their EHRs – both when changing EHR vendors and when receiving clinical information from other providers – and agree that the appropriate exchange of information enhances providers' ability to provide efficient, high-quality care to their patients. However, the proposed regulations implementing the information blocking provision are beyond the scope of the language and intent of the *Cures Act*. Further, the FAH is concerned that, as proposed, the regulations do not appropriately account for the significant time and financial resources that would be required of health care providers as directed by Section 4001 of the *Cures Act*. Section 4001 directed the Secretary of HHS, in consultation with stakeholders, to "establish a goal with respect to the *reduction of regulatory or administrative burdens (such as documentation requirements)* relating to the use of electronic health records" and develop a strategy and recommendations to meet that goal.[11] The list of priorities for that strategy include "activities that provide individuals access to their electronic health information," as well as activities related to protecting privacy and security of electronic health information.[12]

In order to effectively implement the information blocking and burden-reduction provisions of the *Cures Act*, the FAH offers comments and recommendations regarding: the effective date of the proposed regulations; the proposed regulations' interaction with other

[11] 42 USC 300jj-11(a)(1) (emphasis added).
[12] 42 USC 300jj-11(b)(2)(D)–(F).

federal and state laws; the definition of EHI; the proposed exceptions for activities that do not constitute information blocking; recommendations for additional exceptions; and the request for information regarding price information.

Effective Date of Information Blocking Requirements

The Proposed Rule does not explicitly propose an effective date for the information blocking requirements but does state that the Proposed Rule is considered economically significant under Executive Order 12866.[13] As such, any portions of the rule for which there is not an explicitly finalized effective date would become effective 60 days after publication of the Final Rule.[14] It is particularly concerning that ONC effectively proposes that the information blocking requirements, which carry potentially significant penalties, would go into effect *years* before health IT vendors would be required to deliver the technological capabilities to effectively and efficiently provide the information contemplated under the proposed requirements.[15]

Given these effective date considerations, coupled with the complexity of the information blocking proposals and the considerations FAH has raised herein, **the FAH strongly urges ONC to issue a Supplemental Notice of Proposed Rulemaking (SNPRM) to seek additional comments on the information blocking provisions. The FAH also urges ONC to ensure that there is a minimum 18- or 24-month effective date from the date the SNPRM is finalized, depending on the technical difficulties associated with operationalizing the proposals.**

Interaction with HIPAA and Other Federal and State Laws

Congress drafted the information blocking provision and other interoperability-related provisions in the *Cures Act* to complement rather than supplant or upset existing federal and states laws. Specifically, the statute does not alter the underlying structure and force of these other laws, such as HIPAA; federal and state antitrust laws; federal and state laws governing trade secrets and intellectual property; and state laws governing patient privacy and exchange of patient information. **As such, the FAH urges ONC to ensure that the proposed regulations implementing the information blocking provision give full force and effect to the other federal and state requirements and limitations on the exchange of information.**

The statute clearly reflects Congress' intention that the information blocking provision works in concert with – and does not supplant – the structure of these other federal and state laws that establish substantive rights and obligations that govern requests for various types of EHI. For example, the definition of information blocking in Section 4004 of the *Cures Act* contains a

[13] 84 Fed. Reg. 7424, 7588

[14] National Archives and Records Administration, Federal Register Blog, *When does this rule go into effect?*, available at: https://www.federalregister.gov/reader-aids/office-of-the-federal-register-blog/2015/03/when-does-this-rule-go-into-effect.

[15] The proposed implementation date for the transition in certification criteria for EHR technology in the Proposed Rule is 24 months after the final rules effective date, nearly two years after the proposed effective date for the information blocking rules. As noted elsewhere in this letter, the FAH strongly believes that the proposed implementation dates in the Proposed Rule – including those proposed at 24 or 25 months – do not allow sufficient time for health IT vendors and health care providers to comply with the multitude of newly proposed requirements for an uncharted initiative in a very complex environment.

broad exception for practices that are "required by law."[16] Elsewhere in that section, the statute notes that ONC and the Office for Civil Rights (OCR) may refer to the OIG suspected information blocking practices among entities or individuals using certified technology that is technically able to exchange information and "under conditions where exchange is legally permissible."[17] Section 4002 of the *Cures Act* adds conditions of certification regarding the use of APIs to access, exchange, and use health information, including "all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws,"[18] which encompasses both the HIPAA Privacy Rule and state privacy laws. And Section 4006 of the *Cures Act* adds 42 USC 300jj-19(e) – Accessibility of Patient Records – which directs the Secretary and the National Coordinator to promote awareness of individuals' right of access to their protected health information pursuant to the HIPAA Privacy Rule.[19]

HIPAA Privacy Rule

Given the clear statutory directive that regulations implementing the information blocking provision not conflict with or disturb the HIPAA framework, the FAH believes it is important to reiterate key aspects of the HIPAA requirements that govern the individuals or entities that can obtain access to individuals' health information, the purposes for which such information can be shared, the scope of the information that can be shared, and the timeliness for providing patients with access to the information.

Entities / Individuals. The HIPAA Privacy Rule applies to covered entities (and business associates working on behalf of covered entities), including health plans, health care providers, and health care clearinghouses. It also gives individuals (and an individual's designee) a right of access to their own health information.

---

[16] 42 USC 300jj-52(a) – "…the term 'information blocking" means a practice that – (A) *except as required by law* or specified by the Secretary pursuant to rulemaking under paragraph (3), is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information…" (emphasis added).

[17] 42 USC 300jj-52(c)(3) – "**Referral.** The National Coordinator and the Office for Civil Rights of the Department of Health and Human Services may refer to the Inspector General instances or patterns of refusal to exchange health information with an individual or entity using certified electronic health record technology that is technically capable of trusted exchange *and under conditions when exchange is legally permissible"* (emphasis added).

[18] 42 USC 300jj-11(c)(5)(D)(iv) – "has published application programming interfaces and allows health information from such technology to be accessed, exchanged, and used without special effort through the use of application programming interfaces or successor technology or standards, *as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws*;" (emphasis added).

[19] 42 USC 300jj-19(e)(1)(B) – "**Updating education on accessing and exchanging personal health information.** To promote awareness that an *individual has a right of access to inspect, obtain a copy of, and transmit to a third party a copy of such individual's protected health information pursuant to the Health Information Portability and Accountability Act, Privacy Rule (subpart E of part 164 of title 45, Code of Federal Regulations),* the Director of the Office for Civil Rights, in consultation with the National Coordinator, *shall assist individuals and health care providers in understanding a patient's rights to access and protect personal health information under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191),* including providing best practices for requesting personal health information in a computable format, including using patient portals or third-party applications and *common cases when a provider is permitted to exchange and provide access to health information*" (emphasis added).

The *Cures Act* did not expand the universe of entities or individuals that can obtain access to protected health information under HIPAA or the purposes for which such access may be granted. For example, for purposes of health care operations, a covered entity requesting patient information must have or have had a relationship to the patient, and the information must be related to that relationship.[20] This limitation on disclosures for health care operations purposes prevents a covered entity from disclosing protected health information, without the patient's authorization, to an entity whose relationship to the patient is unrelated to the requested health information.

Purposes. As HHS explains in its online *Summary of the HIPAA Privacy Rule*, "A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities."[21] As such, the only required disclosures under the HIPAA Privacy Rule are to the individual and to HHS for compliance or enforcement activities.[22] Other disclosures or uses of identifiable health information by covered entities (and business associates, if permitted or required by its business associate contract[23]) are not permitted unless explicitly delineated in the Privacy Rule, such as disclosures to public health authorities[24] and among covered entities (and/or business associates) for treatment, payment, and health care operations.[25] These regulatory requirements are critical for protecting patients' privacy.

Scope. In addition to defining the circumstances under which uses or disclosures are permitted or required, the HIPAA Privacy Rule also governs the scope of the information that can be shared. For example, a covered entity (or business associate) requesting protected health information from or disclosing such information to another covered entity "must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request" unless the Privacy Rule explicitly states that minimum necessary does not apply (*e.g.*, for treatment purposes).[26] And for health care operations purposes, the protected health information shared between the covered entities must pertain to those entities' relationship with the individual.[27]

---

[20] 45 CFR §164.506(c)(4) – "A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is: (i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or (ii) For the purpose of health care fraud and abuse detection or compliance."

[21] HHS, *Summary of the HIPAA Privacy Rule*, available at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[22] 45 CFR §164.502(a)(2)

[23] 45 CFR §164.502(a)(3) – "**Business associates: Permitted uses and disclosures.** A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement."

[24] 45 CFR §164.512(b).

[25] 45 CFR §164.506.

[26] 45 CFR §164.502(b).

[27] 45 CFR §164.506(c)(4).

The Privacy Rule also explicitly delineates an individual's right of access to his protected health information[28] as contained in the designated record set(s).[29] As HHS explains in its online guidance document *Individuals' Right under HIPAA to Access their Health Information 45 CFR §164.524*, "An individual does not have a right to access PHI that is not part of a designated record set because the information is not used to make decisions about individuals."[30] For example, a hospital might have an incident report concerning staff members' occupational exposure to a particular pathogen carried by a patient. That record would not be part of the patient's designated record set, and it would be inappropriate for a patient to have access to that occupational health record.

Timeliness. The Proposed Rule makes several references to actors operating in a "timely" manner. For example, the proposed regulation at § 170.315(b)(10)(A) states that a single patient EHI export from certified technology must "Enable a user to timely create an export file(s) with all of a single patient's electronic health information the health IT produces and electronically manages on that patient."

The FAH notes that while electronic access to EHI through APIs may enable individuals to access their information in the designated record set more quickly, the *Cures Act* did not amend the timeframe under which a covered entity must provide the individual with access to his protected health information. The HIPAA Privacy Rule requires a covered entity to provide the information within 30 calendar days of receipt of the request, with the opportunity to extend the time by an additional 30 days if the information is not readily accessible within the original 30-day period.[31] This is particularly important with regard to information in the designated record set that is not maintained in an readily accessible format and for which additional time may be required for retrieval.

As described above, the HIPAA Privacy Rule governs, among other things: a) the individuals or entities that can request access to individuals' EHI; b) the purposes for which information can be shared; c) the scope of the EHI that is permitted to be shared among covered entities and business associates; and d) the scope of the EHI that is required to be shared with the individual or the individual's designee. **As such, the FAH recommends additional clarifications to the regulations implementing the information blocking provision, as well as**

[28] 45 CFR §164.524(a)(1) – "**Right of access.** Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for: (i)Psychotherapy notes; and (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."

[29] 45 CFR §164.501 – "Designated record set means: (1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity."

[30] HHS, *Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524*, available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

[31] 45 CFR §164.524(b)(2).

additional exceptions for activities that do not constitute information blocking to ensure this interaction with HIPAA is clear. These are discussed in more detail in the sections below.

Existing Requirements Under Other Federal and State Laws

As discussed above, the statute is also clear that the proposed regulations implementing the information blocking provision do not supplant other relevant federal and state laws that impact the ability of actors to share electronic health information.[32] For example, 42 CFR Part 2 places additional limitations on the disclosure of substance abuse disorder patient records beyond those required by HIPAA. Moreover, HIPAA does not preempt state laws "that are more stringent" than HIPAA,[33] and numerous state laws impose additional limitations on the use and disclosure of health information beyond those imposed by HIPAA. For instance, while HIPAA permits covered entities to disclose protected health information for treatment, payment, or health care operations activities without the explicit consent of the individual, New York law states that health care providers can be liable for professional misconduct for "Revealing of personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient, except as authorized or required by law."[34] A HIPAA preemption analysis performed by the New York State Department of Health (NYSDOH) states that "NYSDOH takes the position that the New York State Public Health Law ("PHL") is NOT PREEMPTED BY HIPAA…" (emphasis in original) and that "…To the extent that State law provides greater privacy for health information or more complete record keeping, State law prevails."[35]

In a number of states, disclosures of various categories of sensitive health information that would be permissible under federal law are only permitted with the consent of the patient.[36] Furthermore, although a disclosure may be clearly permissible under HIPAA, a provider may not be able to determine with any certainty whether that disclosure is permissible under state law. For example, South Carolina provides that certain records that identify a patient with a mental

---

[32] *See* 42 USC 300jj-52(a) – "…the term 'information blocking" means a practice that – (A) *except as required by law*…" (emphasis added). *See also* 42 USC 300jj-52(c)(3) – "…*and under conditions when exchange is legally permissible*" (emphasis added).

[33] HIPAA § 264(c)(2); 45 CFR §160.203(b).

[34] New York State Education Law §6530(23), available at: https://www.health.ny.gov/professionals/office-based_surgery/law/6530.htm.

[35] NYSDOH, *HIPAA Preemption Analysis*, available at: https://www.mssny.org/App_Themes/MSSNY/pdf/Practice_Resources_HIPAA_-NPI_Health_Insurance_Privacy_Rule_Privacy_Preemption_Analysis.pdf.

[36] *E.g.*, La. Stat. Ann. § 40:1081.10 (prenatal and postnatal genetic tests are confidential "unless express written consent to their release is granted by the person tested"); Mich. Comp. Stat. § 330.1748(7)(c) (requiring consent for disclosures of mental health records for operations purposes and limiting disclosures for treatment purposes to those "necessary for treatment"); N.M. Stat. § 24-2B-6(A) (requiring a legally effective release to disclose HIV test results to an individually not specifically authorized to receive the test under the statute); S.C. Code Ann. § 44-22-100 (disclosures of specified mental health records are prohibited without consent except as required by a court or as necessary or required to cooperate with government agencies, to further the welfare of the patient or the patient's family, or to carry out certain provisions of law); Tenn. Code § 33-3-105 (disclosures of confidential mental health information without consent is only permissible as necessary to carry out statutory duties and in other limited circumstances); Utah Code § 62A-15-643 (requiring consent for disclosures of certain mental health records unless ordered by a court or disclosure is necessary to carry out specified statutes); Wis. Stat. § 252.15(3m) (limiting disclosure of an HIV test to specified persons and circumstances without consent).

health diagnosis or substance use disorder for whom commitment to a treatment facility has been sought cannot be disclosed without consent except in limited circumstances, including "when furthering the welfare of the patient or the patient's family."[37] Different providers endeavoring to comply with this state law may take different views as to whether a particular disclosure is prohibited because there is ultimately some ambiguity when this statutory standard is applied to particular facts.

As is currently the case when an activity could be governed by multiple federal or state laws, individuals and entities must evaluate their risk when an activity that is permitted or encouraged under one law is not compliant with another. This is a frequent occurrence for health care providers trying to navigate various state and federal requirements regarding the sharing of protected health information. Compliance with state privacy laws is often determined on a case-by-case basis depending on the totality of the circumstances involved, leading to uncertainty for health care providers regarding whether they are permitted to share the information. While there is an explicit exception in the *Cures Act* for practices that are "required by law,"[38] it may not adequately capture the "grey areas" that providers will inevitably encounter. In these areas, even with the aid of counsel, a provider may determine that a disclosure risks non-compliance with state law but cannot definitively determine whether it is legally required to decline the disclosure request by virtue of those compliance risks.

As discussed in more detail below, the FAH recommends explicitly accounting for such uncertainty in the information blocking exceptions under the Proposed Rule by establishing a "good faith" exception for health care providers who believe that sharing information in a specific circumstance would not comply with other federal or state laws. Such an exception fits within the structure of the *Cures Act's* information blocking definition, which states that a health care provider's action is only information blocking if "such provider *knows* that such practice is unreasonable…"[39] (emphasis added). A health care provider who believes in good faith that sharing the information could result in noncompliance under competing federal or state laws or regulations would not meet this knowledge standard, and it would be inherently reasonable for this individual or entity to engage in a practice that interferes with, prevents, or materially discourages access, exchange, or use of EHI.

In addition to the "good faith" exception, the FAH also urges the Secretary to establish other appropriate state law-based exceptions, as determined through collaboration with states, health care providers, and other stakeholders.

Definition of Actors Subject to the Information Blocking Requirements

Under the *Cures Act*, actors subject to the information blocking requirements include health care providers, health IT developers, health information networks (HIN), and health information exchanges (HIE). In the Proposed Rule, ONC proposes to define each of these categories of actors broadly. For example, the definition of health care provider would include

[37] S.C. Code Ann. § 44-22-100(A)(4).
[38] 42 USC 300jj-52.
[39] 42 USC 300jj-52(a)(1)(B)(ii). *See also* proposed 45 CFR §171.103(c).

virtually every type of health care practitioner and facility provider by using the very broad definition of health care provider established under the HITECH Act.

Expansive Definition of Health Care Provider

This expansive definition is problematic in that many of the practitioner and facility types included in that definition have not participated in the Medicare or Medicaid EHR Meaningful Use Program (renamed the Promoting Interoperability Program (PIP)), which provided initial incentives to acute care hospitals, critical access hospitals and physicians to invest in and implement CEHRT to improve patient care quality and efficiency. While the period of government funding has ended, these providers are held accountable for the continued use of CEHRT via regulatory requirements. Other types of health care providers, such as post-acute care providers of services, behavioral health providers, health care clinics, and a variety of clinicians, have neither been afforded access to nor otherwise benefited from any such investment by the government. In addition, prevalent EHR platforms for some provider types (*e.g.*, skilled nursing facilities) may not be certified or even be offered by a health IT developer of certified health IT that would be subject to the information blocking statute. The FAH is concerned that being omitted from these incentive programs has left many of these other provider types at a significant disadvantage, both with respect to the availability of health IT products that could meet the proposed requirements under this rule as well as the lack of funding and preparation to acquire and implement that health IT. Notably, the statute explicitly provides that "the Secretary shall ensure that health care providers are not penalized for the failure of developers of health [IT] or other entities offering health [IT] to ensure that such technology meets the requirements to be certified under this subchapter."[40] And for those providers that have invested in their own health IT in the absence of any government incentive program, requiring them to change HIT platforms would be infeasible and unreasonably burdensome.

Health Care Providers Penalties Should be Limited to "Appropriate Disincentives"

In the Proposed Rule, ONC notes that a health care provider could also meet the definition of a HIN or HIE under certain circumstances. Section 4004 of the *Cures Act* subjects noncomplying health IT developers, HINs, and HIEs to civil monetary penalties (CMPs) of up to $1,000,000 per violation. In contrast, health care providers are subject to what the statute refers to as "appropriate disincentives" under federal law. The FAH is deeply concerned that, as proposed, a health care provider could potentially face penalties under the CMP authority as well as under the appropriate disincentive authority, contrary to the language and intent of the *Cures Act*. **A health care provider should not be subject to penalties under both of these authorities, and the FAH urges ONC to clarify that insofar as a health care provider is concerned, any practice by that provider that violates the information blocking rule is subject only to enforcement under the appropriate disincentive authority.**

The FAH's recommendations for enforcement of the information blocking requirements, including "appropriate disincentives" for health care providers are discussed in more detail in the Enforcement of the Information Blocking Requirements section below.

[40] 42 U.S.C. § 300jj-52(a)(7).

Health Care Providers are Always Health Care Providers

It is appropriate to narrow the focus of enforcement authority for health care providers to appropriate disincentives because health care providers are responsible for furnishing care to their patients. That is the primary focus of the activity of any provider, and **the FAH recommends that ONC and OIG ensure that entities that are licensed and/or certified to provider health care services are always treated as health care providers for purposes of determining whether an information blocking violation has occurred and the appropriate enforcement mechanism.**

This would apply to all health care providers, even those that may also engage in some activities that could implicate the definition of HIN or HIE. Where an actor is a provider of health care services whose primary purpose is patient care and who also performs some activities that are HIN or HIE activities, that actor should be treated as a health care provider to which the "knowing" standard applies for determining violations and for which the enforcement mechanism is the appropriate disincentive authority. For example, an overly broad application of the terms HIN and HIE could implicate health care providers participating in accountable care organizations (ACOs) and other delivery reform models that seek to improve the quality and efficiency of patient care. An ACO is necessarily involved in the flow of patient information among a number of providers, some but not necessarily all of whom are affiliated with the ACO. The primary purpose of the ACO is to facilitate improved patient care – not to serve the principal function of an HIN or HIE.

The FAH-recommended clarification regarding health care providers is consistent with the general statutory requirement that penalties not be duplicated with respect to an individual or entity involved. **In the case of health care providers, this would mean application of "knowing" standard for determining violations and the appropriate disincentive authority for any actual violations of the information blocking rule.**

Self-Developers

The Proposed Rule supports this view of health care providers always being health care providers for those that develop health IT or a modification to health IT to improve delivery of services to their patients (self-developers). Under the Proposed Rule, a self-developer would not be considered a health IT developer because the self-developer is licensed or certified to provide health care services and its goal is not to derive a source of income from the sale of a health IT product, but rather to improve the quality or efficiency of the delivery of patient care. Thus, the purpose of the self-developer remains providing patient care, not offering its IT products for sale. **The FAH strongly supports the proposal that self-developers would not be considered health IT developers and further recommends that ONC and OIG adopt the recommendations outlined above regarding the treatment of entities licensed and/or certified to provide health care services as health care providers.**

Enforcement of the Information Blocking Requirements

Education, Outreach, and Period of Nonenforcement

Section 4004 of the *Cures Act*, the information blocking provision, seeks to ensure that information that can be or should be exchanged under HIPAA and other relevant federal and state laws is indeed being shared. As discussed above, however, the complex interaction between the information blocking rule and pre-existing state and federal privacy and security laws, as well as other related state and federal laws, and the potential application or nonapplication of the exceptions to the rule (among other concerns) pose the potential for substantial confusion for the wide variety of actors who will be subject to its provisions.

Given the scope and complexity of the information blocking provision and the potentially significant penalties for non-compliance, health care providers, health IT developers, HINs, and HIEs must be given adequate opportunity to learn the new regulations, understand the implications, and develop plans for organizational and individual compliance. Actors may need to modify, or establish new, policies regarding the use and disclosure of patient health information in their control to ensure compliance with the information blocking provision, HIPAA, and other federal and state laws. Organizations and their staff will also need to undertake significant education and training efforts.

The FAH strongly encourages ONC to conduct outreach efforts to health care providers and other actors before the effective date of any information blocking rule. The outreach should include comprehensive, ongoing education initiatives for actors with a focus on practices that would meet the requirements of the exceptions, including specific examples upon which actors could rely. Materials similar to safe harbors should be available to guide actors, and ONC and OIG should respond to inquiries from individual actors that would be anonymized and made available to all relevant stakeholders. As noted earlier, ONC must afford all actors sufficient time to develop and implement revised and new policies for compliance with the information blocking rule as well as to educate and train professionals and staff.

The FAH also strongly urges ONC and the OIG to pursue a nonenforcement policy during at least the first two years following the effective date of the information blocking rule in order to continue the education and outreach campaign suggested above. This period is necessary for actors to develop policies to address the many different situations they may face under this rule. This is especially important for health care providers who face a multitude of different types of requests from different persons and whose ability to share patient health information may be limited by other federal or state laws, or by professional ethics or judgment, based on the particular facts and circumstances of the request for that information. Organizational policies for compliance with the various provisions of the information blocking rule will require refinement over time based on the experience of health care providers in responding to different types of requests. Health care providers should not be subject to potentially significant penalties for inadvertent errors or for situations not envisioned by either the agencies or health care providers during the initial implementation of the finalized version of the Proposed Rule.

CMS and HHS have previously implemented nonenforcement policies when implementing new programs or policies in order to permit individuals or entities additional time to transition to a new set of requirements imposed upon them without fear of facing substantial penalties for inadvertent errors or unintended noncompliance. Periods of nonenforcement are designed to afford the agencies and the regulated stakeholders a smooth transition period during which stakeholders develop a full understanding of the scope of the new requirements and the steps required to come into full compliance with them. It also provides the agencies with regular feedback from and ongoing dialogue with stakeholders about compliance complications and unintended consequences associated with the regulations as initially implemented.

"Appropriate Disincentives" for Health Care Providers

After this initial period of education, outreach, and nonenforcement, the FAH recommends that both agencies adopt a "disincentive" policy for health care providers that emphasizes corrective action over penalties. The statute makes a clear distinction between penalties that may apply for health IT developers, HINs, and HIEs and those that may apply for health care providers. Civil monetary penalties of up to $1,000,000 per violation are authorized for the former,[41] and discretion is given to the Secretary to develop a disincentive approach for the latter.[42] Had Congress intended the Secretary to adopt a civil monetary or other financial penalty approach to disincentivize information blocking practices by health care providers, it would have specifically required that in the law.[43] The statute also directs the Secretary to avoid duplication of penalties established for actors under laws in existence before the enactment of the *Cures Act*.

Given the very broad range of types of health care facilities and practitioners included in the proposed definition of health care provider, and the inexperience of many of those facilities and practitioners with the PIP program, or any similar program, adopting a policy that imposes financial penalties for any violation by any health care provider is unreasonable**. Instead, the agencies should first engage with the health care provider to identify the practice(s) that violated the information blocking requirements and then work with the provider to pursue appropriate modifications to its policies to avoid repeating the error. If the OIG does pursue a policy to impose financial penalties to encourage health care providers to adhere to the information blocking requirements, those penalties should be a last option for the OIG in addressing violations by providers. Additionally, such penalties should only apply to health care providers who, after a corrective action plan process, continue to engage in a pattern of practices that violate the information blocking rule.** Focusing on these "outlier" actors as opposed to trying to police every potential information blocking action is the most efficient use of Agency resources and will have the greatest impact on improving the exchange and use of information.

---

[41] 42 USC 300jj-52(b)(2)(A) – **Developers, networks, exchanges**…shall be subject to a civil monetary penalty determined by the Secretary for all such violations identified through such investigation, which may not exceed $1,000,000 per violation.

[42] 42 USC 300jj-52(b)(2)(B) – **Providers**…appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking.

[43] The bill as passed by the House of Representatives initially adopted a financial penalty approach for health care providers (*i.e.*, the application of a PIP penalty) that was subsequently fundamentally altered before final passage of the *Cures Act*.

With respect to health care providers who participate in the PIPs, if the final rule includes financial penalties as an appropriate disincentive, those penalties should not duplicate the penalties that already exist under the PIPs, as directed by the *Cures Act*. Instead, the penalties should work within the structure of the PIPs, with the amount of any information blocking penalty tailored to the violation involved. Because penalties under the PIPs can be substantial, the agency should evaluate the practice(s) that gave rise to the violation(s) and determine the amount of the penalty as a percentage of the overall PIP penalty. **Any PIP penalty imposed on a health care provider should be reserved for those providers who engage in a pattern of practices that continue to violate the information blocking requirements even after having engaged in a corrective action plan process.**

The FAH also notes that, in the CMS interoperability Proposed Rule, CMS proposes to publicly report those health care providers participating in the PIPs who submitted a "no" response (or did not respond) to any of the three information blocking attestation statements. The policy proposed by CMS in its rule – informing the public (and potential patients) about whether an eligible clinician, acute care hospital, or critical access hospital has engaged in information blocking – is also a clear disincentive to engage in such behavior.

The use of the term "appropriate disincentives" in the statute is also important for its focus on incentives. As noted earlier, only a subset of the potential group of providers under the proposed definition of health care provider have ever received incentives from the government to acquire and implement health IT that meet certain requirements. Post-acute care and behavioral health care providers, as well as a variety of other types of facilities and health care practitioners, have not received any incentives from CMS to help defray the significant costs of investment of health IT to drive improvements in the delivery of care to their patients. **It would be fundamentally unfair to apply a uniform disincentive policy under which penalties that may apply under the PIP program to acute care hospitals, critical access hospitals, and clinicians would also be applied to providers who never participated in or benefitted from that program.**

Finally, the Proposed Rule is silent on the availability of any appeals rights for health care providers and other actors to challenge a determination of the OIG of a violation of the information blocking rule. **The FAH strongly recommends that the final rule both clarify that appeals rights are available for actors and identify for stakeholders the particular provisions of the relevant regulations that afford appeals rights to challenge determinations of information blocking rule violations.**

Definition of EHI

The proposed definition of EHI extends beyond the authority granted to the Secretary in the *Cures Act*.[44] As noted above, Section 4004 of the *Cures Act* (42 USC 300jj-52) defines and

[44] The Proposed Rule would define EHI as "(1) Electronic protected health information; and (2) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of

prohibits activities that are considered information blocking to ensure that EHI that can be lawfully exchanged under HIPAA and other relevant federal and state laws is indeed appropriately shared. The *Cures Act* does not define EHI, however, "EHI" has long been used by ONC and others as synonymous with electronic protected health information (ePHI),[45] and the **FAH believes that the EHI should properly be defined as ePHI with a slight modification to account for information provided by a patient to a health IT developer, HIN, or HIE rather than a provider.**

The FAH urges ONC to largely define EHI as ePHI in accordance with Congress' intent and to avoid unnecessary confusion as to the scope of EHI. The proposed definition of EHI includes both ePHI and "[a]ny other information that [1] identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and [2] is transmitted by or maintained in electronic media that [3] relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."[46] The latter component of the definition of EHI included in the Proposed Rule exactly mirrors requirements for ePHI with two key differences: 1) ePHI excludes certain education and employment records and 2) ePHI is "created or received by a health care provider, health plan, employer, or health care clearinghouse." With regard to the former difference, nothing in the legislative history of the *Cures Act* indicates that Congress intended to target information blocking with respect to education and employment records and ONC does not indicate any concern with employer or education records that are exempt from the definition of ePHI.

With regard to the latter difference, it is true that data of interest for purposes of information blocking may be "provided directly from an individual, or from technology that the individual has elected to use, to an actor covered by the information blocking provisions."[47] For example, if a patient's pacemaker gathers data that is maintained by a health IT developer regulated by the information blocking provision, it would be appropriate to consider that data EHI so that the health IT developer is barred from improperly interfering with the patient's attempt to transmit cardiac and performance data to his or her cardiologist in a standardized and clinically useful format.[48] This circumstance, however, could be simply addressed by defining

---

health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 84 Fed. Reg. at 7601 (proposed 45 CFR §171.102).

[45] *E.g., compare* 42 C.F.R. §495.20(d)(15), (f)(14) *with* §495.22(e)(1), (f)(1) (using the terms EHI and ePHI interchangeably in establishing the protect patient health information objective for meaningful use); 80 Fed. Reg. 62762, 62793 – 95 (Oct. 16, 2015) (using EHI and ePHI interchangeably and establishing requirements regarding security of ePHI for the protect EHI objective); 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003) (using EHI and ePHI interchangeably); 67 Fed. Reg. 53182, 53194 (Aug. 14, 2002) (describing EHI as a subset of PHI).

[46] 84 Fed. Reg. at 7601 (proposed 45 CFR §171.102).

[47] 84 Fed. Reg. at 7513.

[48] Health IT developers are explicitly barred from knowingly interfering with, preventing, or materially discouraging access, exchange, or use of EHI, and health IT developers of certified health IT may be subject to civil monetary penalties for engaging in information blocking. Public Health Services Act §3022(a)(1)(B)(i) & (b)(2)(A), 42 USC §300jj-52(a)(1)(B)(i) & (b)(2)(A). Therefore, defining EHI to include information created or received by a health IT developer of certified health IT ensures that the information blocking provision operates as intended to regulate these entities. In contrast, defining EHI to include information that was neither created by nor received by an entity subject to the information blocking provision unnecessarily includes broad swaths of information (*e.g.*, banking

EHI as "electronic protected health information and information created or received by a health IT developer, HIE, or HIN that would constitute electronic protected health information if it were created or received by a health care provider, health plan, employer, or health care clearinghouse." This approach makes the difference between EHI and ePHI readily apparent and minimizes potential confusion that might arise from the inconsistent interpretation of the two definitions.

The *Cures Act* aims to improve the flow of communications among health care providers with respect to the care they furnish to their patients. A new or overly expansive definition of EHI as applied to health care providers will complicate if not undermine the effectiveness of the information blocking policies Congress enacted, especially when considered across the care continuum of health care providers and patient care settings. As proposed, the definition also raises significant operational issues – including requirements for the access, exchange, and use of types of data and information that current EHR technology does not accommodate. Certain types of communications are not stored in EHRs while other types are held by health care clearinghouses. There is nothing in the language of Section 4004 or any legislative history that indicates congressional intent to extend third party data record repositories to be included in the definition of EHI, unless the entity controlling the repository is itself an actor subject to the information blocking rule.

Except as Required by Law

The definition of information blocking in Section 4004 of the *Cures Act* contains a broad exception for practices that are "required by law." This provision is an independent statutory exception to the information blocking provision, separate and apart from the exceptions created by regulation, as evidenced by the language. The definition of information blocking begins with two separate exceptions clauses – "except as required by law or specified by the Secretary pursuant to rulemaking"[49] (emphasis added). The "or" signifies that actions that fall under either of these types of exceptions – any current laws and regulations or future information blocking-specific regulations[50] would not be considered information blocking for purposes of the statute.

The construction of this language provides unambiguous evidence that Congress intended the information blocking provision to work in concert with – and not supplant – the structure of other federal (*e.g.,* HIPAA) and state laws that establish substantive rights and obligations that govern requests for various types of EHI. **As such, the FAH notes that any action that falls under the "required by law" provision is not information blocking under the statute and does not require a separate regulatory exception.** Thus, for example, if a disclosure is prohibited by a state's privacy law but the actor's failure to make the disclosure does not

---

records reflecting health insurance premium payments) that are not in the possession of any entity subject to the prohibition on information blocking.

[49] 42 USC 300jj-52(a)(1) – "…the term 'information blocking" means a practice that – (A) *except as required by law or specified by the Secretary* pursuant to rulemaking under paragraph (3), is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information…" (emphasis added).

[50] 42 USC 300jj-52(a)(3) – "**Rulemaking.** The Secretary, through rulemaking, shall identify reasonable and necessary activities that do not constitute information blocking for purposes of paragraph (1)."

precisely fit within the requirements of proposed 45 C.F.R. §171.202, the actor's non-disclosure would not constitute information blocking because it is "required by law." The FAH urges ONC to make this distinction clear in future rulemaking related to the information blocking requirements. Additionally, it is within this framework that the FAH offers the below comments and recommendations related to ONC's proposed exceptions and the request for information regarding potential new exceptions.

Proposed Exceptions for Activities that Do Not Constitute Information Blocking

The FAH evaluated the ONC proposed exceptions for activities that do not constitute information blocking in light of the statutory framework discussed above, including that the "required by law" language establishes an independent statutory exception. Given that framework, the FAH recommends several revisions to the proposed exceptions to ensure their alignment with the statute and congressional intent. The FAH also offers several revisions to the proposed exceptions to ensure actors can operationalize the information blocking requirements and exceptions.

Educational Materials and More Specific Guidance for Actors

As discussed elsewhere in this comment letter, the FAH strongly encourages ONC and OIG to conduct outreach efforts to health care providers and other actors with a focus on practices that would meet the requirements of the exceptions, including specific examples upon which actors could rely. Materials similar to safe harbors should be available to guide actors, and the Agency should respond to inquiries from individual actors that would be anonymized and made available to all relevant stakeholders. For example, CMS previously provided such examples in their information blocking attestation guidance to health care providers participating the Merit-based Incentive Payment System (MIPS).[51]

Documentation Burden on Actors to Prove Compliance with the Exceptions

The FAH believes that, as proposed, the regulations do not appropriately account for the significant documentation burden on a health care provider to prove it meets one of the delineated exceptions. These burdens are in direct conflict with Section 4001 of the *Cures Act*, which directs the Secretary of HHS, in consultation with stakeholders, to "establish a goal with respect to the *reduction of regulatory or administrative burdens (such as documentation requirements)* relating to the use of electronic health records" and develop a strategy and recommendations to meet that goal.[52] The list of priorities for that strategy include activities related to protecting privacy and security of electronic health information.[53]

This exceptions section of the Proposed Rule is fatally flawed in that it: does not provide sufficient guidance to actors (*e.g.*, health care providers) regarding the documentation required to

[51] CMS, The Merit-based Incentive Payment System (MIPS) Promoting Interoperability Prevention of Information Blocking Attestation: Making Sure EHR Information is Shared, 2019 Performance Year, *at* https://qpp-cm-prod-content.s3.amazonaws.com/uploads/487/2019%20MIPS%20Promoting%20Interoperability%20Fact%20Sheet.pdf.
[52] 42 USC 300jj-11(a)(1) (emphasis added).
[53] 42 USC 300jj-11(b)(2)(D)–(F).

meet the exceptions; and, in some instances, puts forth requirements for which it would be extremely difficult, if not impossible in some instances, for the health care provider to even document compliance.

The Proposed Rule places the onus on the actor (e.g., health care provider) to prove compliance with an exception at all times but is silent on the documentation required to prove such compliance. Thus, a health care provider could think it has the appropriate documentation but later the ONC and OIG could determine the documentation is lacking based on some previously unknown standard. **It is patently unfair to hold health care providers and other actors to unknown documentation standards, particularly when the onus is on the actor to defend itself from an allegation of information blocking and when the actor is faced with potentially significant penalties. Quite simply, health care providers cannot be expected to comply with overly vague or unknown requirements.**

In addition to the unknown documentation standards, it is also unfair to hold health care providers to requirements with which it would be difficult – or impossible – to comply. For example, to meet sub-exception 1 under the Promoting Privacy of EHI exception (exception number 2), an actor could not encourage an individual to refuse to provide the consent or authorization required by another federal or state law. To meet this sub-exception, it is likely that a health care provider will develop a policy (or amend a current policy) to handle preconditions imposed by other laws, including a process to confirm and document the individual's consent. That policy would likely also include guidance to clinicians and other staff that they cannot encourage an individual to refuse to provide consent or authorization. In that instance, would the organizational policy meet the documentation requirement? Or would additional documentation be required? If the latter, it is unclear how a health care provider would otherwise document that no clinicians or other staff members encouraged an individual to refuse to provide consent. It is also unclear how a clinician responding to a patient's questions about sharing information – including a discussion of the pros and cons of providing that information – would be viewed by ONC and OIG should there be an accusation of information blocking.

The FAH agrees that health care providers and other actors should not unduly influence an individual's decision regarding consent. However, clinicians and other providers should not be discouraged from answering patient questions or engaging in appropriate conversations about an individual's health record. Additionally, health care providers should not face impractical or impossible documentation requirements.

To ameliorate these concerns, the FAH strongly urges ONC to provide examples of the documentation needed under each exception. In addition, if there is not a reasonable opportunity for a health care provider to document compliance – or if the documentation required is overly burdensome – then the exception must be amended to provide such an opportunity and/or reduce the burden or removed entirely.

The FAH offers the following comments regarding the seven proposed exceptions to the information blocking provision.

1. Preventing Harm (45 C.F.R. § 171.201)

The FAH appreciates ONC's recognition that health care providers may sometimes delay providing – or even refuse to provide – information to other health care providers – or to patients themselves – in order to prevent harm to a patient or other individual. To ensure this exception appropriately protects patients and the providers that serve them, the FAH urges ONC to specifically include "emotional harm." In CMS guidance on the information blocking attestation for MIPS, CMS provided an example of a clinician holding a patient test result for a short period of time to allow the clinician to tell the patient the result directly.[54] Clinicians are in the best position to determine if their patient is likely to experience harm (including emotional harm) from seeing – and perhaps misinterpreting – a test result before the clinician has an opportunity to speak with the patient; they should not be put in a situation where taking the appropriate action(s) to protect their patient(s) results is at odds with the information blocking requirements.

The FAH also notes that there are technological limitations that would prevent health care providers from complying with the proposed exception. Specifically, most current technology is not capable of the data segmentation necessary to hold back only a portion of the patient record (*e.g.*, information related to a substance use disorder) while providing the remainder of the requested information. Additionally, current technology is unable to "scrub" the rest of the patient record to pull out other data (*e.g.*, a specific medication or procedure) that could implicate the sensitive information that was held back. **Given these limitations, the FAH urges ONC to hold off on implementing the data segmentation requirement until the technology improves.**

2. Promoting Privacy of EHI (45 C.F.R. § 171.202)

The FAH appreciates ONC's recognition of the need to protect the privacy of an individual's EHI. ONC proposes that actors can only meet this exception through one of the four identified methods (sub-exceptions) delineated in the Proposed Rule. The sub-exceptions are: 1) a precondition imposed by law not satisfied; 2) health IT developer of certified health IT not covered by HIPAA; 3) denial of an individual's request for their ePHI in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3); and 4) respecting an individual's request not to share information.

As discussed at length above, the *Cures Act* does not supplant HIPAA or other federal or state laws. And, also discussed above, the "as required by law" language in the Act is an independent statutory exception to the information blocking provision. **Evaluated in that light, the FAH believes that, as proposed, the privacy exception is out of alignment with the *Cures Act,* HIPAA, and potentially other federal and state laws.** For example, HIPAA still governs who can obtain access to such information and for what purposes, the scope of such

[54] CMS, The Merit-based Incentive Payment System (MIPS) Promoting Interoperability Prevention of Information Blocking Attestation: Making Sure EHR Information is Shared, 2019 Performance Year, *at* https://qpp-cm-prod-content.s3.amazonaws.com/uploads/487/2019%20MIPS%20Promoting%20Interoperability%20Fact%20Sheet.pdf.

information, and the timelines for providing that information. Regarding the purposes for which such information can be shared, the HIPAA Privacy Rule contains only two required disclosures: to the individual, and to HHS for compliance or other enforcement activities. Other disclosures by covered entities are not permitted unless explicitly delineated in the Privacy Rule. Also important is the scope of the information that can be shared among covered entities (and business associates), such as the HIPAA "minimum necessary" requirement for disclosures other than for treatment purposes. It is therefore concerning that the Proposed Rule envisions sharing information for non-treatment purposes that would go beyond the "minimum necessary," making it impossible for health care providers' to comply with both the information blocking and HIPAA requirements. **The FAH urges ONC to amend its privacy exception to recognize that the information blocking provisions are meant to work within the structure of HIPAA and other federal and state laws, not override them. The FAH also urges ONC to make clear that any action that falls under the "required by law" language is not information blocking under the statute and does not require a separate regulatory exception.**

For entities that operate across multiple jurisdictions, it is operationally challenging to tailor their information exchange practices to each state's privacy laws. **The FAH appreciates ONC's recognition of these challenges and urges the Agency to include an accommodation in sub-exception 1 for health care providers that adopt "organization-wide privacy practices that conform with the most restrictive privacy laws regulating their business."**[55]

Lastly, related to the documentation burden discussion above, the FAH urges ONC to clarify that the requirements of proposed section 171.202(b)(2) are met where a provider makes its standard consent or authorization form (*i.e.*, release of medical records form) available on its public website and upon patient request. As drafted, proposed section 171.202(b)(2) suggests that the provider bears the burden to endeavor to secure any required consent or authorization from the patient when faced with a request from a third party. Instead, the entity (including a third-party application) requesting the information should be responsible for obtaining the required consent or authorization. For example, if a third-party application is requesting access to EHI on behalf of a patient, that application should be required to obtain the patient's legally effective authorization and to supply proof of such authorization to the health care provider from which the application is requesting the EHI. If the application does not provide such proof, then the health care provider would, appropriately, not provide the data under this sub-exception. To require the health care provider to seek to obtain such consent is inefficient and overly burdensome, particularly considering that the provider may not have interacted with the patient in years and may not have his updated contact information. This inefficiency would in turn lead to delays in individuals accessing their data while the provider tries to reach the individual or handle a potentially high volume of requests requiring preconditions. Moreover, if a provider were obligated to contact patients to secure an authorization based on a third-party inquiry, the provider would effectively be marketing that third-party to its patients, raising additional privacy concerns. By making its release of medical

[55] 84 Fed. Reg. at 7528. "In order to ensure that the information blocking provision does not diminish the privacy rights of individuals being serviced by such actors, we are considering the inclusion of an accommodation in this sub-exception that would recognize an actor's observance of a legal precondition that the actor is required by law to satisfy in at least one state in which it operates."

records form publicly available, a provider has done all things reasonably necessary within its control to provide the patient with an opportunity to authorize the disclosure, and any additional outreach would be unreasonably and potentially improper.

3. Promoting Security of EHI (45 C.F.R. § 171.203)

As proposed, in order to fit within this exception, a practice undertaken by a health care provider or other actor must meet all three conditions delineated in the Proposed Rule, including that the practice is directly related to safeguarding the confidentiality, integrity, and availability of EHI. Additionally, an actor's organizational policy must be based on a security risk assessment that aligns with at least one consensus-based standard.

The FAH is concerned that, as proposed, this exception could be read as reactive to security events rather than encouraging a proactive security culture. As described in the Proposed Rule, ONC appears to be requiring that a health care provider's security policies be linked to a clear security threat, but it is unclear whether that is a threat that has already occurred (and thus the security policy was put in place to prevent a second such occurrence) or one that *could* occur. **The FAH urges ONC to clarify the exception to ensure the latter is applicable, as health care providers must be empowered to take a proactive security stance, including designing and implementing policies for potential future security threats. The FAH also notes that health care providers and other actors should not have to meet all three conditions, as it is infeasible to comply with such a requirement for all current or potential future security threats.** New security threats are emerging daily and spreading rapidly, much more quickly than the security industry can keep up with them. As such, most emerging threats do not have practices for health care providers and other actors to follow, requiring their security professionals to improvise and rely on their experience. Health care providers should not be faced with a situation in which protecting the security of their systems and their patients' medical records puts them at odds with the information blocking requirements.

In addition, as discussed in more detail in Section VI of this letter, the FAH is deeply troubled by the privacy and security concerns raised by unvetted third-party applications. **The FAH strongly believes that all applications seeking to connect to a health care providers' APIs must undergo the vetting process outlined in Section VI and that providers and API vendors that refuse to connect to non-vetted applications should not be considered "information blocking."**

4. Recovering Costs Reasonably Incurred (45 C.F.R. § 171.204)

As proposed, the definition of EHI would include non-observational health data (*e.g.*, patient risk scores, quality improvement data) if that data is identifiable to the patient. This is troubling for health care providers, as it would appear to permit entities to request this provider-created data that is outside of the scope of the USCDI and may be outside the scope of the designated record set under HIPAA. Also troubling is that, as proposed, this provider-generated data, which may involve proprietary algorithms, would have to be provided to the requesting entity at cost. The FAH strongly disagrees with the proposal to require health care providers to share this provider-generated and potentially proprietary non-observational health data, as well

as the proposal to do so at cost. **The FAH urges ONC to implement information blocking exceptions for EHI that is outside of the USCDI for provider-to-provider sharing and outside of the electronically maintained portion of the HIPAA designated record set for provider-to-patient sharing to help alleviate these concerns.**

The Proposed Rule prohibits health care providers from charging fees to individuals to electronically access their EHI and distinguishes this from the cost-based fees covered entities may charge for copies of ePHI under HIPAA. This proposal is out of alignment with HIPAA and the *Cures Act.* As discussed at length above, the proposed definition of EHI includes ePHI, and the *Cures Act* did not supplant HIPAA. As such, this information would fall under the HIPAA regulations, which permit cost-based fees for access to ePHI.

The Proposed Rule also appears to permit API Technology Suppliers to charge API Data Suppliers (*e.g.,* health care providers) for access to the API, but prohibits those suppliers from charging third-party applications for access to the API. There are often significant resources involved in providing an individual's health record, and health care providers will see increased requests with the use of the FHIR API and the proliferation of third-party applications. The FAH is concerned about these applications continually using the health care provider-funded API for access to patient data – free of charge and for their own benefit (rather than the patient's benefit) – resulting in bandwidth issues and placing an undue burden on health care providers. The FAH has long supported the rights of individuals to access their health data and continues to do so. Third-party applications, however, are not necessarily acting for the individual and should not have free, unfettered, access to health care providers' systems to collect patient data for their own gain. **As such, the FAH urges ONC to revisit these proposals and strike an appropriate balance between third-party application access to the API and the financial and resource burden placed on health care providers.**

5. Responding to Requests that are Infeasible (45 C.F.R. § 171.205)

The FAH supports ONC's proposed exception for circumstances where "complying with [a] request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances," but urges ONC to clarify that this condition is satisfied by an actor's good-faith belief that the burden is unreasonable, taking into account the listed factors. Although the substantiality or insubstantiality of the burden associated with a request may be readily evident in some cases, there will be closer cases where an actor should satisfy this condition for the exception based on its good-faith belief. This is particularly true where the actor is a health care provider because under the information blocking standard applicable to providers in the statute, a health care provider only engages in information blocking where it "knows that [a] practice is unreasonable."[56]

Moreover, where a health care provider faces a substantial burden in responding to a request based on limitations on the interoperability of health IT over which the provider has little control, the health care provider should be able to request a reasonable alternative from the health IT developer instead of providing such an alternative itself. Where a health care provider does not have sufficient control over the relevant technology, the

[56] 42 U.S.C. § 300jj-52(a)(1)(B)(ii).

development of a reasonable alternative may itself be infeasible and requiring such a reasonable alternative in such a situation would make this necessary exception illusory. Importantly, Congress instructed the Secretary to ensure that providers "are not penalized for the failure" of other entities to ensure that technology meets health IT certification requirements.[57] Where providers face a substantial burden in responding to a request, this often flows from limitations on the interoperability of health IT products over which the provider has little control (*e.g.*, imaging tools that do not export data to the certified EHR), and the exception for requests that are infeasible should recognize this reality.

Recommendations for Additional Exceptions

The FAH believes there is a significant need for additional exceptions to ensure the information blocking requirements and exceptions align with the statutory language and Congressional intent that these provisions work with – as opposed to override – HIPAA and other federal and state laws. For example, exceptions related to the scope of information shared among providers and between providers and patients are necessary to ensure that: the information being shared is that which is needed for clinical purposes or required under HIPAA; all actors are aware of the requirements and what information must be shared; and that such information can be exchanged without undue burden in accordance with the direction to reduce regulatory burden in Section 4001 of the *Cures Act*.

Provider-to-Provider EHI Disclosures

To carry out the intent of Section 4004, a specific exception is necessary to determine the scope of information shared during provider-to-provider EHI disclosures. Such an exception should clarify that, for provider-to-provider exchanges, a provider does not engage in information blocking when it limits the EHI disclosed to the data classes and elements established under the United States Core Data for Interoperability (USCDI) standard and takes reasonable steps to provide any additional EHI that is specifically requested. In other words, actors would not be "information blocking" if they do not share information beyond the scope of the USCDI in response to a typical provider inquiry. Using the USCDI will ensure that all actors are aware of the information that is required to be exchanged and focus on that information most relevant to providing the best clinical care to patients in a timely manner – and available through certified health IT.

In updating the criteria to which health IT vendors must build and certify their products, ONC proposes to replace the Common Clinical Data Set (CCDS) with the USCDI standard to increase the minimum baseline of data classes commonly available for interoperable exchange. Further, ONC proposes a process for future expansion of the USCDI that includes providing stakeholders the opportunity to comment on the USCDI's expansion, increasing transparency and ensuring a wider range of stakeholder input. In a regulatory environment where failure to share information is potentially subject to financial penalties, it is important to establish certainty that the information required to be shared can be captured and shared using certified health IT. It would also substantially reduce burdens on health care providers so their time and resources can be focused on delivering efficient and quality patient care.

[57] *Id.* at § 300jj-52(a)(7).

As the USCDI standard focuses on accessing, exchanging, and using data elements for clinical care, and the capability will be required of certified health IT, it is the logical benchmark for information required to be shared via provider-to-provider exchanges. In the CMS Interoperability Proposed Rule, CMS also supports the use of the USCDI among certain health insurance plans and believes it will improve care coordination and reduce administrative burdens. Specifically, CMS notes that "…use of the USCDI to exchange information furthers care coordination" and that "…the USCDI standard contains many of the data points required to more effectively coordinate care."[58] Using the USCDI standard will also prevent requesting providers from being burdened with a surfeit of information that must be sorted through to identify information pertinent to the treatment of the patient's present disease, injury, or condition. To furnish the right clinical care at the right time, which may be on an urgent or emergency basis, the relevant patient health information to provide that care must be made available promptly and be easily consumable by the health care provider. Lastly, focusing on the USCDI would provide certainty for actors regarding the scope of information that must be shared. **As such, the FAH strongly recommends that ONC develop and finalize an additional exception for information outside of the USCDI for provider-to-provider EHI disclosures.**

Provider-to-Patient EHI Disclosures

A specific exception is also necessary to determine the scope of information shared during provider-to-patient EHI disclosures. Such an exception should clarify that, for provider-to-patient exchanges, EHI is limited to the electronic data contained in the designated record set, as established under HIPAA. In other words, health care providers would not be "information blocking" if they do not share information with the patient beyond the scope of the designated record set. Focusing on the designated record set is consistent with the law and will ensure that health care providers and patients are aware of the information that is required to be exchanged.

As discussed above, the HIPAA Privacy Rule explicitly states that an individual has a right of access to his PHI as contained in the designated record set, and the *Cures Act* did not supplant other federal or state laws, including HIPAA. As such, the FAH strongly recommends that ONC develop and finalize an additional exception for information outside of the designated record set for provider-to-patient EHI disclosures.

Good Faith Compliance Exception for Non-Clinical Disclosures

Also discussed above, individuals and entities must evaluate their risk when an activity that is permitted or encouraged under one federal or state law is not compliant with another. Health care providers must frequently navigate these concerns when dealing with the morass of state and federal requirements regarding the sharing of EHI in its various forms. For example, state privacy laws are not usually binary, meaning there is not an easy "yes" or "no" answer to determining compliance; instead compliance is dependent on the specific circumstances involved, and providers' decisions are usually guided by an evaluation of the regulatory risks rather than a legal opinion that an activity is absolutely prohibited or required. These "grey

[58] Fed. Reg. at 7640 (March 4, 2019).

areas" cause tremendous uncertainty for health care providers, even with the assistance of counsel, and should be included in the exceptions provided in the Proposed Rule.

As noted above, there is an explicit exception in the *Cures Act* for practices that are "required by law,"[59] but it may not adequately capture the "grey areas" caused by the vagaries of state laws. If a health care provider believes that a disclosure otherwise required under the information blocking provision risks non-compliance with a non-binary state law, the provider should not be considered an "information blocker." **To provide such protections, the FAH recommends establishing a "good faith" exception for health care providers that believe that sharing information in a specific circumstance would risk non-compliance under other federal or state laws.** This exception fits squarely with the information blocking definition, which states that a health care provider's action is only information blocking if "such provider *knows* that such practice is unreasonable…."[60] A health care provider who believes in good faith that sharing the information could result in noncompliance under competing federal or state laws or regulations would not meet this knowledge standard.

In addition to the "good faith" exception, the FAH also urges the Secretary to establish other appropriate state law-based exceptions, as determined through collaboration with states, health care providers, and other stakeholders.

Price Estimator Tool Exception

In light of the Request for Information (RFI) on price information and the broad definition of EHI proposed by ONC, the FAH is concerned that "information blocking" may be broadly construed to require providers that create price estimator tools to disclose the data produced by those price estimator tools to third parties. The FAH recognizes that patients have a strong interest in clear, accurate, and actionable information on their estimated cost-sharing obligations for anticipated care – whether that is used by the patient for financial planning purposes or to aid in their selection of a provider, and to that end, supports the development of patient-focused price estimator tools. As proposed, however, there is a risk that the information blocking rules could be read to apply to the cost-sharing estimates provided to patients by providers. Subjecting price estimator tools to regulation through the information blocking rules could have the perverse effect of chilling innovation at the precise time when promising, private-sector solutions to price transparency issues are emerging. **Therefore, the FAH strongly urges ONC to expressly adopt an exception exempting the data produced by price estimator tools from the information blocking requirements.** This exception would foster innovative, private-sector solutions that respond to a key priority of the Secretary without adding to the burdensome regulations health care providers already face.

Price Information Request for Information

The FAH continues to be supportive of efforts to ensure that consumers have access to clear, accurate, and actionable information concerning their copayment, coinsurance, and deductible (collectively, "cost-sharing") obligations, and its members are actively engaged in the

[59] 42 USC 300jj-52.
[60] 42 U.S.C. §300jj-52(a)(1)(B)(ii) (emphasis added); s*ee also* proposed 45 CFR §171.103(c).

development and implementation of improved price estimator tools, both independently and in coordination with payers. The FAH is concerned, however, that ONC is considering prematurely regulating innovation around price information and price transparency in ways that stifle innovation and increase compliance costs while underestimating the technical challenges around price estimator tools, failing to target the appropriate range of actors (*e.g.*, payers), limiting regulatory experimentation at the state level, and interfering with competition in a significant portion of the United States' economy. **The FAH, therefore, urges ONC to allow space for price transparency practices to develop among providers and payers before considering any regulation or guidance in this area.**

EHI Does Not Include Price Information

Including price information within the scope of EHI for purposes of information blocking would run contrary to Congress' clear intent and would be technically infeasible where payers are largely excluded from information blocking rules. The information blocking provision of the *Cures Act* has its genesis in ONC's Report to Congress on Health Information Blocking[61] (hereinafter Information Blocking Report). In that report, ONC described and analyzed five hypothetical scenarios to illustrate how its proposed criteria for information blocking could be applied in real-world situations that reflect actual information blocking anecdotes. Each scenario involved the transmission, disclosure, or use of clinical information, particularly orders, laboratory tests, and patient health records.[62] At no point in the report did ONC indicate that information blocking could occur with respect to non-clinical information, including pricing information (*e.g.*, the reimbursement rate or discount negotiated between a provider and a payer, the allowed amount applied by the payer, or the patient's estimated cost sharing obligation). Likewise, nothing in the text or legislative history of the *Cures Act* indicates that Congress intended to address the handling of non-clinical information. In fact, the Information Blocking Report and the resulting statute both focus explicitly and *exclusively* on the activities of health IT developers, HIEs, HINs, and health care providers. Conspicuously missing from this list of entities subject to information blocking rules are insurers, third party administrators, health plans, and other payers, indicating that Congress did not intend to address price transparency issues through information blocking rules.[63] As a result, the information blocking statute cannot be used to require a payer that is not acting as an HIN or HIE to provide information on a covered individual's cost-sharing obligations (*e.g.*, the individual's remaining deductible obligation) in a standardized or usable format.

The FAH urges ONC to properly confine information blocking to interference with the access, exchange, or use of EHI for clinical purposes in accordance with Congress' intent. Although payers – insurers, group health plans, third party administrators, Medicare, Medicare Advantage organizations, and others – are not generally subject to the prohibition on information blocking, they are best suited to provide clear, accurate, and actionable coverage and cost-sharing information for all providers and suppliers involved in an episode of care. Payers can provide this information to members and beneficiaries without

[61] ONC, Report to Congress on Health Information Blocking (Apr. 2015), available at https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.
[62] *Id.* at Appx. A.
[63] 42 USC §300jj-52(a).

jeopardizing price-based competition among providers. They are also uniquely qualified to provide patients with precise information concerning any limitations on their coverage, the scope of patient cost-sharing obligations (including out-of-pocket spending limits, deductibles, coinsurances, and any reference-based pricing strategies used by the plan), any network tiering used by the plan, and the applicable allowed amount for each provider or supplier involved in an episode of care. And because an episode of care typically involves multiple providers and suppliers, the payer is the only entity that can provide a patient with an accurate and actionable estimate of their potential financial exposure for the entire episode of care. Seeking this information from each provider and supplier involved in an episode of care is not only inefficient, but it is also error-prone because the cost-sharing picture is fragmented among the providers and suppliers and may not accurately reflect the details of the patient's coverage.

Moreover, the FAH maintains that general pricing information should not be considered EHI and that ONC lacks regulatory authority to specify the types of pricing information presented to patients. Even if EHI is defined to include individually identifiable electronic information related to the past, present or future payment for the provision of health care to an individual per proposed 45 CFR § 171.102, this data would consist of claims, billing, and collections data for an individual for services rendered (*i.e.*, the types of data that are the subject of HIPAA's administrative simplification requirements at 45 CFR Part 162). It would not include abstract pricing information or responses to hypothetical patient inquiries.[64] Moreover, the information blocking statute prevents providers from interfering with, preventing, or materially discouraging access, exchange, or use of EHI, 42 USC 300jj-52(a), but it does not require a provider to develop EHI that does not otherwise exist (*e.g.*, by synthesizing the results of a patient-specific query of a payer concerning cost-sharing responsibilities with non-EHI concerning the negotiated rate with a payer or similar proxy data). Accordingly, any requirement that particular data be generated in response to patient inquiries or prior to the furnishing of a scheduled service simply does not fit within the information blocking framework created by ONC in its 2015 Information Blocking Report and adopted by Congress in the *Cures Act*.

Impact of Public Pricing Information on Competition

The FAH opposes treating pricing information as EHI subject to information blocking requirements in light of the significant and unpredictable competitive impacts of

[64] Through HIPAA, Congress expressly sought to "encourag[e] the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information," including information that relates to "the past, present, or future payment for the provision of health care to an individual." HIPAA § 261 (purpose); Social Security Act § 1171(4), 42 USC §1320d(4) (added by HIPAA § 262) (definition of "health information"). In doing so, however, Congress was unconcerned with generalized information (*e.g.*, payer fee schedules, general clinical protocols, etc.) and was instead focused on information relating to the condition of or care provided "to an *individual*" (*e.g.*, test results and claims data, whether de-identified or individually identifiable). *See* Social Security Act § 1171(4). To achieve its purpose, Congress charged the Secretary with adopting standards for transactions to enable health information to be exchanged electronically. Social Security Act § 1173(a)(1), 42 USC §1320d-2(a)(1) (added by HIPAA § 262). Congress' focus on the transmission of payment information rather than generalized price information is clear from the list of statutorily specified transactions, which includes transactions with respect to health claims or equivalent encounter information, health claims attachments, enrollment and disenrollment in a health plan, eligibility for a health plan, health care payment and remittance advice, health claim status, and referral certification and authorization. Social Security Act § 1173(a)(1), 42 USC §1320d-2(a)(1) (added by HIPAA § 262).

the resulting disclosures. In requesting information on price information, ONC suggests making pricing information broadly available on public websites. Such a practice would run contrary to guidance from the Department of Justice (DOJ) and FTC concerning the sharing of pricing information. Economists and antitrust enforcers have long recognized that the disclosure of negotiated provider network rates could discourage and distort competitive price negotiations. In fact, the DOJ and FTC's antitrust safety zone for pricing surveys specifically cautions against the use of current pricing data.[65]

There is a distinct benefit to ensuring that patients only receive an estimate of their patient cost-sharing amounts and information concerning a provider's financial assistance and charity care programs rather than more general information concerning the negotiated rates between the provider and the payer. **Providing more generalized information concerning the payer-provider relationship instead of focusing on patient-specific information increases the likelihood that competitively sensitive pricing data will be aggregated from price estimator queries, creating unexpected and anti-competitive market distortions in the name of transparency.[66] Moreover, if negotiated rates for all plans were made available on a public website, as suggested in the RFI, this sensitive pricing data would be readily available without the need for aggregation, immediately altering the managed care market to the detriment of consumers.** The *Sherman Act*, which prohibits restraints on trade (including price fixing) has been in place for over 125 years, and Congress did not intend to limit competition and upend settled rules concerning the sharing of competitively sensitive pricing information when it targeted clinically harmful information blocking practices in the *Cures Act*.

Operational Concerns and Pricing Information

Although hospitals are increasingly focusing on providing clear, actionable, and accurate cost-sharing information to patients on request, particularly for frequently utilized procedures and services, they face significant operational challenges in doing so. First, the managed care agreements between payers and hospitals can be complex and non-standard. Second, there are thousands of procedures, services, and items that might be provided during an inpatient or outpatient hospital stay in any number of potential combinations, and the innumerable potential combinations of services and payers presents a significant barrier to providing price estimation tools for the full range of hospital items and services. Finally, in most cases a hospital will not have adequate information to provide any reasonable price estimate unless and until the time of

[65] Department of Justice and Federal Trade Commission, Statement on Provider Participation in Exchanges of Price and Cost Information (Aug. 1996). Potential harm to competition might also arise from disclosures of pricing information in connection with referrals. ONC asks whether, for example, health IT developers should be required to include a mechanism for providers to have access to price information connected with referrals. This process, however, would create the potential for current rates to be shared between two competitors where, for example, the referring provider and the receiving provider offer some of the same services, but the receiving provider also offers some additional advanced diagnostic or treatment modalities. The creation of such a mechanism could be used by a competitor to gain access to confidential pricing information, to the detriment of competition.

[66] Notably, Congress recognized the importance of maintaining the confidentiality of competitively sensitive information when it expressly prohibited HIPAA administrative simplification standards from requiring "disclosure of trade secrets or confidential commercial information" unless otherwise required by law. 42 USC §1320d-1(e). It would be improper for the information blocking provision to be used to effectively impose standards that require the disclosure of competitively sensitive information in light of the HIPAA prohibition on such standards.

pre-registration, when the patient provides coverage information, the hospital receives the physician order or referral, and the payer responds to an eligibility verification request.

Standardized disclosure requirements for price information would be complicated by the enormous variability in the managed care rate structures negotiated between providers and payers. Some agreements may adopt a simple fee schedule, but others might base payment on diagnosis related groups (DRGs), with or without additional payments for outlier cases; a percent of charges, with or without a cap; value-based payment structures; per diems; or a number of other payment structures. **Requiring providers to present information on such disparate payer contracts in a standardized manner would be unnecessarily burdensome, would detract from the relevant patient cost-sharing information, and could have unintended effects on the market as providers and payers are pressured to negotiate basic fee schedules in lieu of value-based or other innovative payment arrangements.** The assumption that this contractual pricing data could be converted to a standardized format like a fee schedule is simply inconsistent with the reality of managed care contracting for facility services. In fact, some hospitals have found that it is cost-prohibitive and technically unworkable to translate the actual rates in managed care agreements into a standardized data set and keep them up to date (particularly where the agreement does not use a simple fee-for-service rate structure). The FAH understands from its members that are developing or have developed price estimator tools that the standardization of data in managed care agreements is simply not a viable option. Regulation in the vein envisioned by the RFI would hamper pragmatic, private-sector innovation around this data problem by requiring that providers focus their efforts around an impractical, unduly burdensome approach to price transparency.

In addition, a provider's ability to develop a reasonably accurate price estimate depends in part on the provider receiving (1) accurate and complete coverage information from the patient, (2) an order or information concerning the anticipated hospital services, and (3) accurate and standardized cost-sharing information from the payer. Hospitals generally do not obtain the first two pieces of information until pre-registration for scheduled services and may not have this information until after services are furnished (as in the case of emergency are and unscheduled inpatient care). It is also worth noting that the anticipated services may differ substantially from the care ultimately received.[67] The estimated patient cost-share for a particular inpatient hospital procedure may under- or over-estimate the length of stay and the actual bundle of services that will ultimately be provided to the patient. These differences can be particularly marked where a patient suffers an unforeseen complication that necessitates additional services and increases the patient's cost-sharing liability. With regard to the third category of data needed for a patient cost-sharing estimate, if the patient provides accurate coverage information, the payer should respond to the provider's inquiry with current data on the patient's cost-sharing responsibilities and limits. However, because payers are not subject to information blocking requirements unless acting as an HIN or HIE, this information may not be provided in a standardized format that can be easily integrated into a patient price estimator tool. **Therefore, providers may be unable to**

[67] By way of example, there is enormous variation in the services provided to maternity patients, who may or may not ultimately require anesthesia, surgical intervention, an inpatient stay in excess of two midnights, and a wide range of other health care items and services. Any cost-sharing estimate offered during the pre-registration process (or prior to discharge) would necessarily rely on assumptions concerning the patient's care that are unlikely to reflect the patient's actual experience.

provide reasonably accurate price estimates outside of the context of scheduled services and, even then, may face significant operational difficulties in responding to patient requests for price estimates.

Notably, even when price estimates can be generated, the estimates will be limited to the provider's own services and may therefore underestimate the patient's overall financial exposure for an episode of care. For example, the professional fees for the surgeon and anesthesiologist may not be included in a price estimate from a hospital, particularly a hospital that does not employ physicians. **As discussed above, the payer is best-suited to provide a more complete picture of the patient's likely financial exposure resulting from an episode of care, taking into account all of the relevant suppliers and providers.**

Surprise Billing

The FAH generally shares ONC's interest in reducing or preventing surprise medical billing. The FAH and its members are currently working with key congressional committees and engaging with numerous state legislatures to develop legislative strategies to protect patients from surprise medical bills. **As information blocking does not contribute to surprise billing, and Congress and state legislatures are working to develop legislative solutions, the FAH does not believe surprise billing falls within ONC's authority or otherwise implicates the information blocking provisions in the *Cures Act.***

Price Transparency Initiatives Should Focus on Consumer Priorities

The FAH maintains that the information blocking provision of the *Cures Act* is not the appropriate vehicle for addressing price transparency issues. But the FAH is committed to helping patients understand their cost-sharing and believes that such information should reflect the values and the interests of actual patients. In the experience of our members, relatively few patients indicate an interest in obtaining pricing information, and where they seek this information, patients are largely focused on obtaining cost-sharing estimates for financial planning purposes rather than comparison shopping purposes. Moreover, patients show little interest in the amount a third-party payer will reimburse the provider, and instead are focused on their own copayments, coinsurance, and deductible obligations. Therefore, there is little patient benefit to be derived from providing any information other than an estimate of the patient's expected cost-sharing obligation, and the provision of additional, unnecessary information creates significant risks of market distortions and patient confusion.

Along similar lines, the FAH believes that information concerning "the Medicare rate" for a service is not a useful reference point and does not help patients to understand their potential cost-sharing. Medicare rates are not negotiated in arm's-length transactions and provide little to no information about the rates negotiated with or established by other payers, let alone the cost-sharing borne by the patient. In addition, the provision of Medicare-specific pricing information by providers would likely create confusion among patients who are either not enrolled in Medicare or who receive their Medicare benefits through a Medicare Advantage plan that pays a different, negotiated rate.

Conclusion on Price Information RFI

For the foregoing reasons, the FAH believes that ONC lacks the authority to subject price estimates and other pricing information contemplated in the RFI to the information blocking rules. Generalized pricing information (*e.g.*, negotiated rates with payers) does not qualify as EHI itself because it is disconnected from payment for the provision of health care to an individual. Further, the information blocking rules cannot be applied to compel a provider to synthesize non-EHI (*e.g.*, contracted rates) with EHI (*e.g.*, coverage information for an individual) to generate price estimate data.

The FAH, however, supports ONC's goal of ensuring that patients have access to clear, accurate, and actionable cost-sharing information. **In order to foster innovation around price estimator tools, the FAH urges ONC to clarify that price estimates are not subject to information blocking rules or to adopt an exception for price estimates (as discussed in section entitled "Recommendations for Additional Exceptions").** Private-sector innovation in this space is ongoing and may wholly obviate the need for federal price transparency legislation or regulations. If federal action is ultimately necessary or prudent, this private-sector-led process would provide Congress and regulatory agencies with additional, critical experience and information concerning price transparency initiatives, the interests of consumers, and ancillary effects of such initiatives on the marketplace.

IX. Request for Information: Registries

As directed by Section 4005 of the *Cures Act*, ONC is seeking to use standards, particularly an API using FHIR Release 4 to improve the interoperability and bidirectional exchange of data between EHRs and registries.

The FAH strongly supports the use of a standards-based API, particularly FHIR Release 4, to reduce the current burden involved in using multiple health IT tools to extract information from one registry or system and then reformat that information to send to a different registry or system. These impediments to information sharing are prevalent with public health registries, as different states have different requirements for the type of information they want submitted, as well as the format for that information.

X. Request for Information: Patient Matching

The FAH appreciates ONC's and CMS's commitment to improving patient matching and agrees with other stakeholders that the lack of a unique patient identifier (UPI) has significantly hindered efforts in this area. **The FAH supports the use of a UPI but recognizes that Congressional action is needed to permit the use of federal funding to adopt and implement a UPI.** In the absence of such Congressional action, the 2017 ONC Patient Matching Algorithm Challenge[68] was a good first step in identifying the current techniques employed for patient matching operations. More must be done, however, to catalyze the advancement and wide-spread deployment of top-tier tools.

[68] HHS Press Release, *HHS Names Patient Matching Algorithm Challenge Winners* (Nov. 21, 2017), available at: https://www.hhs.gov/about/news/2017/11/08/hhs-names-patient-matching-algorithm-challenge-winners.html.

To address patient matching concerns, the FAH encourages ONC and CMS to convene stakeholders from across the industry to develop a private sector-led strategy with government support. As recommended in an industry-stakeholder paper in 2018, this strategy would involve a "neutral coordinating organization" to determine the "standards-based infrastructure to improve patient matching."[69] The Agencies could then support the widespread adoption of the standards-based infrastructure through their regulatory authority. The FAH believes such an approach would reduce the current variability in patient matching capabilities within each local system and exchange.

In addition to the AHIMA paper discussed above, the FAH encourages ONC and CMS to carefully consider recommendations from other organizations that have studied the current deficiencies in patient matching. An October 2018 report from The PEW Charitable Trusts provides several recommendations for near- and long-term actions to improve patient matching. For example, the report discusses opportunities to improve patient demographic data by capturing patients cell phone numbers and email addresses, as well as opportunities to reduce the variation in recording demographic data by adopting the U.S. Postal Service standard for addresses.[70]

****

The FAH appreciates the opportunity to comment on the Proposed Rule. We look forward to continued partnership with ONC and CMS as we strive to advance the use of health IT to improve our nation's health care system. If you have any questions regarding our comments, please do not hesitate to contact me or a member of my staff at (202) 624-1500.

Sincerely,

[69] Journal of AHIMA, *Advancing a Nationwide Patient Matching Strategy* (July-August 2018), available at: http://bok.ahima.org/doc?oid=302539#.XLdByjBKiUk.

[70] The PEW Charitable Trusts, *Enhanced Patient Matching is Critical to Achieving Full Promise of Digital Health Records* (Oct. 2018), available at: https://www.pewtrusts.org/-/media/assets/2018/09/healthit_enhancedpatientmatching_report_final.pdf.