The Office of the National Coordinator for Health Information Technology (ONC) has released a final rule implementing provisions of the 21st Century Cures Act (Cures) related to electronic health information blocking, interoperability and the ONC Health IT Certification Program (Cert Program). Concurrently, the Centers for Medicare & Medicaid Services (CMS) issued a final rule on patient access to data and interoperability. Work on these rules has been directly overseen by senior Administration officials, including the U.S. Department of Health and Human Services (HHS) Secretary Azar.

Provisions in these rules regarding information blocking and application program interfaces (APIs) will impact interoperability and the way data is exchanged between patients, physicians, payers, technology developers, and other health care stakeholders. The rules also promote patient access and price transparency. Together, these rules signal a major push by the Administration to remove all barriers it has identified as impeding patient access to data, and to greatly expand access for payers and third-party companies.

The AMA provided extensive comments on ONC and CMS' proposals. This document provides a summary of HHS' regulation and includes an overview of where AMA's comments impacted the final rule.

HHS Final Rule on Electronic Health Information Blocking, Interoperability and the Cert Program

In the final rule, HHS defines key terms, including electronic health information (EHI) and health information network/exchange (HIN/HIE); (2) discusses activities that would be likely to interfere with access, exchange, or use of EHI; (3) codifies compliance with the information blocking provisions as a Condition of Certification for health information technology (health IT) developers; (4) creates eight exceptions to the general prohibition on information blocking; and (5) modifies health IT developer product development and testing and imposes limitations on business practices, including contracts and fees.

Information Blocking: Cures defines information blocking broadly as any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI when the entity knows it is likely to do so. Cures directs HHS to identify actions that would not be considered information blocking. HHS has created eight exceptions to information blocking: preventing harm; promoting the privacy of EHI; maintaining the security of EHI; recovering costs reasonably incurred; responding to requests that are infeasible; licensing of interoperability; maintaining and improving health IT performance; and limiting the content and manner of an actor's response to EHI requests. Each of these exceptions are complex. ONC describes "actors" regulated by the information blocking provision as: health care providers (with providers defined broadly); health IT developers of certified health IT; and HIN/HIEs.

HHS' policies will also impact any actor that creates, accesses, or exchanges EHI as part of its business model. For all actors under the final information blocking policies, it will be crucial to develop transparent and non-discriminatory organizational policies and data governance frameworks that address the criteria set forth in the exceptions described below. We anticipate that these provisions will require updates to existing contracts and agreements between physicians and other businesses or entities that may or may not be considered actors.

HHS' Final Rule is not meant to require disclosure of EHI in a way that would be impermissible under the Health Insurance Portability and Accountability Act (HIPAA). Yet, if an actor is permitted to disclose EHI under HIPAA, then they are now required to do so to avoid potential information blocking violations—subject to the exceptions described below. Physicians will need to examine existing agreements, policies and procedures, and business practices to consider how these may need to change considering the information blocking rules.

The HHS Office of the Inspector General (OIG) has both investigatory and enforcement authority over information blocking and may issue civil money penalties ($1,000,000 per incident) for information blocking conducted by certified health IT developers and HIN/HIEs. OIG has yet to release its regulation around civil money penalties. Physician penalties will also be established in future HHS rulemaking. HHS is postponing the enforcement of information blocking regulations on all actors for six months after the rule is officially published.

The AMA commented that HHS should reduce the complexity of its proposed information blocking regulation. However, we expect the final rule's information blocking requirements will impose a significant burden on many physician practices. Information blocking requirements are layered on top of existing HIPAA regulations, which are already complex. Many physician practices may require consultants, attorneys, or support from several organizations to understand the full impact of these rules. The AMA is identifying several approaches where our advocacy efforts and education centers can be most effective.

Definition of HIN/HIE

HHS considers an HIN/HIE to mean an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI:

1. Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and
2. That is for a treatment, payment, or health care operations purpose, as such terms are defined in HIPAA regardless of whether such individuals or entities are subject to the requirements of HIPAA.

The AMA commented that HHS should narrowly define HIN/HIE to include entities that facilitate the exchange of EHI in a clinical setting. HHS has excluded language that, in its proposed rule, caused confusion. Specifically, HHS removed the term "substantially influences" to address concerns about possible ambiguity. HHS has also added further clarification to its interpretation of Cures language. HHS clarifies that in order to meet the definition of an HIN or HIE, the entity must enable the exchange of EHI among more than two unaffiliated parties (beyond the HIN or HIE itself). This change is intended to ensure that parties that act as intermediaries in essentially bilateral exchanges—for example, an intermediary that receives EHI from one party in a non-standardized format and converts it to standardized data for the receiving party—would not be an HIN or HIE for information blocking purposes. HHS also states that it believes most, but not all, HIN/HIEs currently function as a covered entity or business associate under the HIPAA Rules. These classifications reflect AMA comments. HHS has also clarified that physicians owning an exchange or network would not themselves be considered an HIN/HIE but rather a "health care provider" with respect to situations that involve their behavior as a health care provider.

Definition of EHI

HHS revised its proposed definition of EHI to mean electronic protected health information (ePHI) as defined in HIPAA, to the extent that ePHI would be included in a designated record set. Consistent with HIPAA, exceptions include psychotherapy notes or information compiled in anticipation of litigation. The

definition of EHI neither includes nor excludes price information. Instead, actors must identify whether price information is included in a designated record set at the time of the request for EHI. De-identified data is excluded from the definition of EHI.

From six months after publication through the 24-month implementation deadline, the scope of EHI subject to the information blocking prohibition will be limited to only data types described in the U.S. Core Data for Interoperability (USCDI)—outlined below. After 24 months, EHI will be considered ePHI.

The AMA commented that HHS' definition of EHI was overly broad, would add confusion to actors seeking to facilitate the access, use, and exchange of EHI, and would increase the burden on physicians and patients. We asked HHS to constrain EHI to the USCDI and provide physicians an information blocking exception for instances where they could not provide EHI based on issues outside their control. HHS' final rule reflects AMA concerns and balances the need for increased access to patient data with adding parameters on how and actors should respond to EHI request. HHS' finalized glide path from the USCDI to ePHI is an important and necessary change from its original proposal.

Examples of Practices Likely to Interfere with Access, Exchange, or Use of EHI

To clarify the scope of the information blocking provision, HHS points to its proposed rule, which outlined several types of practices that HHS believes are likely to interfere with access, exchange, or use of EHI. The examples include:

- Restrictions on access, exchange, or use of EHI through formal means (e.g., contractual restrictions) or informal means (e.g., ignoring requests to share EHI);
- Limiting or restricting the interoperability of health IT (e.g., disabling a capability that allows users to share EHI with users of other systems);
- Impeding innovations and advancements in access, exchange, or use of health IT-enabled care delivery (e.g., refusing to license interoperability elements to others who require such elements to develop and provide interoperable services)*;
- Rent-seeking and other opportunistic pricing practices (e.g., charging fees to provide interoperability services that exceed actual costs incurred to provide the services); and
- Non-standard implementation practices (e.g., choosing not to adopt relevant standards, implementation specifications, or certification criteria).

**An "interoperability element" includes hardware, software, technologies, rights or services that are necessary to access, exchange or use EHI and are controlled by the actor who receives a request for the EHI.*

Exceptions

HHS has defined eight exceptions for actors (i.e., physicians, EHR vendors, HINs/HIE) to explain which practices impacting the access, exchange, or use EHI will not be considered information blocking. If an actor's practice does not meet the all of the conditions of an exception, it will not automatically constitute information blocking. Instead, such practices will be evaluated on a case-by-case basis to determine whether information blocking has occurred.

The AMA commented that HHS should consider the complexity of its information blocking exceptions and their impact on small and solo physician practices. We sought to include a provision within each exception that would allow physicians, based on their professional judgement, to restrict the access, use, or exchange of EHI without being considered information blockers. We believe that without a clear "hold harmless" exception, physicians may resort to hiring consultants and attorneys to wade through each

exception, sub-exception, and condition in order to know which one or group of exceptions apply to each specific circumstance. Requiring physicians to create new policies and procedures and to document each time an exception is used will be onerous. We believe HHS' final set of exceptions are still too complex and more should be done to reduce burden on physicians. The AMA is considering requesting additional sub-regulatory guidance to improve clarity, as well as possible regulatory or legislative fixes.

Preventing Harm Exception – When will an actor's practice that is likely to interfere with the access, exchange, or use of EHI in order to prevent harm not be considered information blocking? This exception recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of EHI. *It will not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.*

An actor must meet all the following conditions:

- The actor must hold a reasonable belief that the practice will substantially reduce a risk of harm;
- The actor's practice must be no broader than necessary;
- The actor's practice must satisfy at least one condition from each of the following categories: type of risk, type of harm, and implementation basis; and
- The practice must satisfy the condition concerning a patient right to request review of an individualized determination of risk of harm.

Privacy Exception – When will an actor's practice of not fulfilling a request to access, exchange, or use EHI in order to protect an individual's privacy not be considered information blocking? This exception recognizes that an actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws. *It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy, provided certain conditions are met.*

To satisfy this exception, an actor's privacy-protective practice must meet at least one of the four sub-exceptions:

- Withholding EHI on the basis that a state or federal privacy law imposes a precondition for providing access, exchange or use of EHI (e.g., a requirement to obtain a patient's consent before disclosing the EHI);
- Entities that are not covered by HIPAA or a business associate but are still certified health IT developers. (e.g., direct-to-consumer health IT provider may meet the second sub-exception if a practice promotes the privacy interests of an individual);
- Denial of an individual's request for ePHI consistent with the HIPAA Privacy Rule's "unreviewable grounds" (e.g., certain requests made by inmates of correctional institutions, information created or obtained during research that includes treatment, and denials permitted by the federal Privacy Act); and
- Respecting an individual's request not to provide access, exchange, or use of EHI.

Each of these sub-exceptions requires having and disclosing organizational policies to support these criteria to the individuals and entities that use the actor's product or service before they agree to use them. HHS states that generally "if an actor is permitted to provide access, exchange, or use of EHI under the HIPAA Privacy Rule (or any other law), then the information blocking provision would require that the actor provide that access, exchange, or use of EHI so long as the actor is not prohibited by law from doing so...."

Security Exception – When will an actor's practice that is likely to interfere with the access, exchange, or use of EHI in order to protect the security of EHI not be considered information blocking? This exception is intended to cover all legitimate security practices by actors but does not prescribe a maximum level of security or dictate a one-size-fits-all approach. *It will not be information blocking for an actor to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.*

Actors can meet this exception if their security practices are:

- Directly related to safeguarding the confidentiality, integrity, and availability of EHI;
- Tailored to specific security risks; and
- Implemented in a consistent and non-discriminatory manner.

In addition, the security practice must be part of an organizational security policy or be based on particularized facts and circumstances that demonstrate that the practice is necessary to mitigate a security risk and that there are no reasonable and appropriate alternatives to the practice.

Fees Exception – When will an actor's practice of charging fees for accessing, exchanging, or using EHI not be considered information blocking? Under the Fees Exception, actors may recover certain costs reasonably incurred for the access, exchange, or use of EHI that HHS believes are unlikely to present information blocking concerns. Fees may result in a reasonable profit. The exception excludes certain fees, such as those based on electronic access to EHI by the individual. *It will not be information blocking for an actor to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met.*

To qualify for this exception, fees must meet the following conditions:

- Meet the basis for fees conditions –
    - For instance, the fees an actor charges must:
        - ◊ Be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;
        - ◊ Be reasonable related to the actor's costs of providing the type of access, exchange, or use of EHI; and
        - ◊ Not be based on whether the requestor or other persons is a competitor, potential competitor, or will be using the EHI in a way that facilitates competitor with the actor.

- And not be specifically excluded.
    - For instance, the exception does not apply to:
        - ◊ A fee based in any part on the electronic access by an individual, their personal representative, or another person or entity designated by the individual to access the individuals EHI; or
        - ◊ A fee to perform an export of EHI via the capability of certified health IT.

If an actor is a health IT developer, the actor must also comply with all relevant conditions of certification.

Infeasibility Exception – When will an actor's practice of not fulfilling a request to access, exchange, or use EHI due to the infeasibility of the request not be considered information blocking? This exception recognizes that legitimate practical challenges may limit an actor's ability to

comply with requests for access, exchange, or use of EHI. An actor may not have—and may be unable to obtain—the requisite technological capabilities, legal rights, or other means necessary to enable access, exchange, or use. *It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met.*

The practice must meet one of the following conditions:

- Uncontrollable events: The actor cannot fulfill the request for access, exchange, or use of EHI due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.
- Segmentation: The actor cannot fulfill the request for access, exchange, or use of EHI because the actor cannot unambiguously segment the requested EHI.
- Infeasibility under the circumstances: The actor demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances.

The actor must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.

Licensing Exception – When will an actor's practice to license interoperability elements in order for EHI to be accessed, exchanged, or used not be considered information blocking? According to the Licensing Exception, an actor's practice to license interoperability elements for EHI to be accessed, exchanged, or used will not be considered information blocking if the practice meets certain timing requirements and licensing conditions. The actor must begin license negotiations with the requestor within 10 business days from receipt of the request and negotiate a license within 30 business days from receipt of the request. Royalties and terms of the license also generally must be reasonable and non-discriminatory, in accordance with specified licensing conditions. *It will not be information blocking for an actor to license interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met.*

Health IT Performance Exception – When will an actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of EHI not be considered information blocking? This exception recognizes that for health IT to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that health
IT be taken offline temporarily. Actors should not be deterred from taking reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of health IT. The actor's practices must be related to the maintenance and improvement of health IT (e.g., temporary unavailability of data or degradation of the performance of health IT). Actors should also be allowed to protect the resiliency of their computer network if third-party applications negatively impact the performance of their systems. These practices must last no longer than necessary. *It will not be information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.*

An actor may take action against a third-party app that is negatively impacting the health IT's performance, provided that the practice is:

1. For a period of time no longer than necessary to resolve any negative impacts;
2. Implemented in a consistent and non-discriminatory manner; and
3. Consistent with existing service level agreements, where applicable.

If the unavailability is in response to a risk of harm or security risk, the actor must only comply with the Preventing Harm or Security Exception, as applicable.

Content and Manner Exception – When will an actor's practice of limiting the content of its response or the manner in which it fulfills a request to access, exchange, or use EHI not be considered information blocking? This exception provides clarity and flexibility to actors concerning the required content (i.e., scope of EHI) of an actor's response to a request to access, exchange, or use EHI and the manner in which the actor may fulfill the request. Under this new exception, an actor's practice of limiting the content of its response or the manner in which it fulfills a request to access, exchange, or use EHI will not be considered information blocking if the practice meets both a "content condition" and "manner condition." Under the content condition, an actor may respond to a request to access, exchange, or use EHI by providing the data elements in the USCDI for 24 months following the final rule's publication date. Under the manner condition, an actor must respond in the manner requested unless technically unable to respond or agreeable license terms cannot be reached, in which case it must respond in an alternative manner. *It will not be information blocking for an actor to limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided certain conditions are met.*

The AMA commented on the need for an exception to address instances where physicians could not provide the entire set of EHI to a requestor. HHS' inclusion of a new "content and manner" exception reflects AMA's advocacy efforts to add additional protections for physicians. For instance, if a physician is asked to provide EHI that their EHR is not capable of supplying or if the request is for EHI using technology a physician does not have, the physician will not be considered an information blocker as long as they provide the EHI they actually have access to and in a format agreed upon between the physician and requester. We believe this is an important exception for physicians who are limited by their EHR vendor's ability to access, use, or exchange patient information.

<u>Changes that impact certified health IT (e.g., EHRs) development, testing, and vendor contracts</u>

API: An application programing interface (API) is a set of software code, protocols and tools that allows unrelated software programs to communicate with one another. APIs act as bridges between two applications, allowing data to flow regardless of how each application was originally programmed or designed. In health care, data sets can have different technical structures and the meaning of data (i.e., data vocabularies and terminology) may not be consistent between health IT products—making interoperability between applications challenging. Because APIs are points of communications between systems, APIs can be developed to simplify interoperability to provide physicians, patients, and other data more efficiently.

HHS includes a new API certification criterion, new standards and implementation specifications, and new Conditions and Maintenance of Certification Requirements for health IT developers, specifically:

- APIs must use the Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) standard, along with a set of implementation specifications;
- Certified APIs need to implement the Substitutable Medical Applications, Reusable Technologies (SMART) Application Launch Framework Implementation Guides (based on the OAuth 2.0 security standard);
- APIs must provide access to and search capabilities for all data elements proposed as part of the USCDI for a single patient and multiple patients;
- APIs must provide an application registration process to help ensure secure connections that include authentication and authorization capabilities;

- Certified API Developers (defined below) must support API-enabled services for data on a single patient and multiple patients; and
- Certified API Developers must publish the terms and conditions applicable to their API technology.

HHS defines several new API technology roles: Certified API Developer (a health IT developer of certified API technology aka EHR vendor); API Information Source (a health care organization/physician that deploys the API technology); and an API User (persons and entities that use or create software applications that interact with API technology). Of note, HHS explicitly includes third-party app developers and payers in their definition of API User. HHS also enumerates permitted and prohibited fees related to APIs and circumstances where they can be assessed. HHS notes that fees charged by API Information Sources may implicate information blocking provisions.

HHS changed the minimum available data requirements for interoperable exchange required for EHR certification. Certification now requires that EHRs meet USCDI standards, replacing the previously used Common Clinical Data Set (CCDS). The USCDI is a standardized data set that includes "clinical notes," allergies, and medications among other important clinical data to help improve the flow of electronic health information and ensure that the information can be effectively understood when it is received. Of note, "clinical notes" is comprised of several types of notes, including consultation notes, discharge summaries, and progress notes.

New API certification criterion for 2015 Edition certified EHR technology supports two use cases: a patient's access to his or her own data and population-level access to a group of patients' data (such as a physician's patient panel, or all patients participate in particular health plan). The core functionality currently required is "read" and not "write", meaning that, for now, applications will be able to pull data from but not necessarily push it back to the EHR—although HHS envisions requiring "write" functionality in the future. APIs must offer the following functionalities: data response; search support; application registration; secure connection, authentication, and authorization (leveraging OpenID Connect Core). Patients should have "persistent access" to their health information without having to re-authenticate for a proposed minimum period of three months. Certified API Developers must develop, test, certify and make APIs available to their customers within 24 months of the final rule's effective date. HHS is also requiring API Information Sources (i.e., physicians) to deploy new APIs in production within the same 24 months of the final rule's effective date.

The AMA supported many of HHS' proposals around APIs and modifications to certified EHR technology. Several of the final rule's provisions will improve physicians' experiences with EHRs and will better protect physicians from excessive fees to connect their EHRs to clinical registries and HIEs. The inclusion of SMART technology will allow physicians to have more choice in which apps they use to interface with EHRs---providing a better user experience. The USCDI increases the amount and utility of patient information to which physicians and patients will have access. EHR vendors must also provide physicians more detail on the fees they do charge and what capabilities their EHRs support "out of the box". EHR vendor contract limitations restrict vendors from blocking physicians from publicizing concerns about their EHR's performance and restricts vendors from requiring physicians use or connect to proprietary technology. HHS' regulation requires EHR vendors to provide support to physicians who wish to switch EHR products and restricts EHR vendors from employing anti-competitive practices. EHR testing and requirements around vendor transparency and product usability have also been improved.

Application Registration and Vetting: Applications (apps) must register with an authorization server. This is a basic technical requirement and not a review process for privacy, quality, or any other substantive criteria. HHS has clarified that any practice of reviewing third party applications must not violate information blocking rules and made it clear that certified health IT developers cannot institute any

vetting process for applications that facilitate patient access to EHI. In response to comments about security concerns, HHS stated that the implementation of technical specifications such as OpenID Connect and OAuth 2.0 allow for secure API deployment, and that otherwise "there is little protection software can provide to protect against nefarious Actors posing as legitimate health facilities."

The AMA provide substantial comments on app registration, third-party access to patient information, and concerns with downstream privacy issues. While the AMA fully supports patients accessing their health information and believes APIs will help patients and physicians better use medical information, the way HHS structured its proposal promoted the desires of third-parties, data brokers, and large technology companies above the needs of individuals. We identified several areas where HHS' policies would enable the monetization of patient information. We commented that this would drive third parties to use information blocking and other HHS policies to access and use patients' information without their knowledge. We cautioned this could significantly impact patients' privacy and their trusted relationships with their physicians. The AMA offered several practical solutions, including requiring EHRs to check if an app was conforming to industry data privacy/security standards and data use best practices. HHS' final rule stopped short of making the necessary changes to protect patient privacy. The AMA will continue to work with policymakers to ensure patients are protected and physicians have confidence in the digital health tools they use or recommend to their patients. We are considering near- and long-term actions at the regulatory and legislative levels to address this critical issue.

Additional API details

- Standard: FHIR is the underlying standard to enable API access. HHS is requiring the use of the US FHIR Core Implementation Guide specifications.
- Data Elements: Health IT developers must make available a certain set of FHIR resources that correspond to the USCDI within 24 months after the rule's effective date.
- Transparency: Health IT developers must make publicly accessible their API technical documentation, including implementation specifications and information about any unique technical requirements required for access. Documentation must be publicly available via a hyperlink and cannot be behind a paywall or any type of registration requirement.
- Conditions of Certification: Health IT developers are required to make their business documentation transparent. Specifically, developers' terms and conditions, including fees, registration process requirements, and any limitations or obligations of application developers will need to be openly published via a public hyperlink. This goes into effect six months after the rule's effective date.
- Fees: HHS finalized a general prohibition on imposing fees associated with API technology, unless the fee arrangement falls within a specific permitted category. Permitted fees must be based on objective and verifiable criteria, uniformly applied across applications vying for API access, and must be reasonably related to the cost of supplying, maintaining, and upgrading the API. Fees may not be predicated on an application's status as a competitor to the vendor. Any usage fee associated with patient access is prohibited.
- Intellectual Property and Right to Access: Health IT developers will need to grant API users all rights that are reasonably necessary to access and use API technology in a production environment. Users should not have to pay a fee in order to license the rights to use the API, nor submit to any provisions regarding exclusivity or limiting competition.

Relating to API fees, the AMA supports HHS' efforts to address excessive fees charged by EHR vendors to connect their products with other health IT systems, health information exchanges, and third-party applications. Some specific fee limitations may reduce excessive costs. Yet, we are concerned the overall framework is complex and has limited usefulness for physicians. We believe HHS' fee structure will ultimately designate physicians as the default revenue stream for EHR vendors and app developers. For

instance, EHR vendors cannot charge app developers or any other entity using APIs, and instead EHR vendors are only permitted to charge physicians. This could result in physicians facing unexpected costs to support API use unrelated to clinical use or patient care.

U.S. Core Data for Interoperability: HHS removed the CCDS definition and its references from the 2015 Edition and replaced it with the USCDI v1 standard. Starting six months after the rule's effective date, all actors, in compliance with the information blocking rule, are expected to provide the USCDI if requested. If the USCDI is not available, actors may use one or more information blocking exceptions. Health IT developers will need to update their certified health IT within 24 months of the rule's effective date to support the USCDI for all certification criteria affected by this change. New required data classes and data elements include:

- Data provenance;
- Clinical notes (includes multiple note types);
- Address & phone number; and
- Pediatric vital signs.

ONC intends to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion. Information on the USCDI expansion process is forthcoming.

EHI Export: HHS acknowledged that switching EHR systems is a time consuming and expensive activity for physicians and that it is difficult for patients to access their EHI. To address this, HHS will require health IT developers to provide the capability to electronically export all EHI they produce and electronically manage in a computable format. HHS will require EHR vendors to implement this requirement within 36 months of the final rule's effective date. The EHI export certification criteria requires that all EHI produced and electronically managed by a developer's health IT be readily available to export for a single patient upon request for his or her health data, and for all patients when a physician seeks to change health IT systems. It further requires health IT developers to provide the format, such as a data dictionary or export support file, for the exported information to assist the receiving system in processing the EHI without loss of information or its meaning to the extent reasonably practicable using the developer's existing technology.

Conditions and Maintenance of Certification: HHS created several Conditions of Certification with accompanying Maintenance of Certification Requirements: information blocking; communications (i.e., "gag clauses"); APIs; real world testing; attestations; and future EHR reporting criteria for submission. These requirements are specific to certified health IT developers, i.e., EHR vendors.

Health IT developers must provide assurances to HHS that they will not take any action that constitutes information blocking or any other action that inhibits the exchange, access to, or use of EHI. Violations by health IT developers of any of these requirements would be subject to ONC direct review, corrective action, and enforcement. A health IT developer's certified health IT may also be subject to its certification being suspended or terminated. HHS includes a new enforcement option that would bar a health IT developer's products or modules from the ONC Cert Program if one or more of its health IT products were found by ONC or an ONC-Accredited Certification Body (ONC-ACB) to be non-conformant with the Cert Program, or if their certification were suspended or terminated. This would effectively block that health IT developer from participating in the Cert Program. HHS created a process for health IT developers to appeal and be reinstated.

Communications: HHS acknowledges there are current vendor practices that limit health IT users from openly discussing or sharing their health IT usage experiences, commonly referred to as "gag clauses."

HHS has created a new Condition of Certification to protect certain communications and communicators. 60 days after the rule's effective date, health IT developers will be precluded from prohibiting or restricting any communication, irrespective of the form of the communication or the identity of the communicator, if the communication is within the range of "protected subject areas."

Health IT developers will be prohibited from restricting communications that are related to:

- The usability of the health information technology;
- The interoperability of the health information technology;
- The security of the health information technology;
- Relevant information regarding users' experiences when using the health information technology;
- The business practices of developers of health information technology related to exchanging electronic health information; and
- The manner in which a user of the health information technology has used such technology.

HHS notes that developers prohibit or restrict communication through contract, such as non-disclosure agreements or other contractual terms, and conduct, including punitive or retaliatory actions against the users of health IT. Health IT developers must issue a written notice to all customers and those with which it has contracts or agreements containing provisions that contravene these requirements annually, beginning in calendar year 2020. The notice must state that any communication or contract provision will not be enforced by the health IT developer. Health IT developers must update contract language that contravenes this Condition of Certification to remove or void any contractual provision whenever the contract is next modified for other reasons or renewed. The rule provides that users may publish screenshots or video of health IT, so long as they are unaltered and are limited in number (screenshots) or length (video) to communicate about one or more of the six protected subject areas.

HHS defines "protected subject areas" as:

- A health IT technology's usability, interoperability, or security;
- The manner in which the users have used the technology;
- The users' experience; and
- Any business practices of health IT developers related to the exchange of EHI.

Health IT developers would be permitted to impose narrow prohibitions on communications that:

- Are made by their own employees;
- Disclose non-user-facing aspects of the software;
- Infringe on the developer's intellectual property rights so long as the communication was not made in "fair use" of the health IT;
- Are unfaithful reproductions of health IT screenshots; and
- Are made during "beta" testing or unreleased product development.

Real World Testing: HHS includes a Condition of Certification that requires health IT developers to annually submit real world testing plans and retrospective test results that include interoperability criteria. HHS states the objective of the testing is to verify that the health IT continues to be compliant with certification criteria, is exchanging EHI in the care and practice settings for which it is intended, and that EHI is received and used by the technology.

Standards Version Advancement Process: HHS will allow health IT developers to choose among the versions of standards and implementation specifications listed in regulation or, alternatively, National Coordinator-approved newer version updates for any or all standards applicable to criteria subject to real

world testing requirements. This is intended to allow health IT developers to migrate their products to new standards' versions in a more rapid pace.

Quality Reporting: ONC is aligning its quality reporting criterion with that of CMS' Quality Program requirements. Health IT developers will be required to implement CMS' Implementation Guide for Quality Reporting Document Architecture Category I for eligible hospitals and Category III for eligible clinicians. This will replace certification to the HL7 Quality Reporting Document Architecture (QRDA) I & III Implementation Guide requirements.

Electronic Prescribing: ONC is aligning its Cert Program's electronic medication prescribing (eRx) criterion with that of CMS' Part D eRx and medication history standards requirement and to facilitate prescription drug monitoring program (PDMP) support. Health IT will be required to adopt the National Council for Prescription Drug Programs' (NCPDP) SCRIPT Standard Implementation Guide v2017071 within 24 months of the rule's effective date.

Data Segmentation: HHS will allow health IT developers to voluntarily adopt new data segmentation for privacy (DS4P) standards. As an optional certification criterion, health IT could be developed to enable a user to create (and receive) a summary record formatted in the consolidated clinical data architecture (C-CDA) standard that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on the re-disclosure.

The AMA promoted the use of data segmentation technology in our comments and requested that all EHRs be required to conform to DS4P. Data segmentation is a vital set of technologies and processes that allow sensitive health information to be shared while protecting patient confidentiality and consent. HHS states that it recognizes the importance of data segmentation to protect patient privacy but refrained from requiring EHRs to support this needed feature. The AMA is involved with several medical specialties to drive the adoption of data segmentation. We will continue to work with several stakeholders and policymakers to ensure that patients can trust that their sensitive health information will be shared safely and security and that physicians will have access in compliance to state and federal law.

<u>Timeline for interoperability, information blocking, and EHR changes</u>

60 days after publication the rule's general effective date.

- Certain conditions of EHR vendor certification go into effect, including prohibiting vendors from blocking physicians from openly discussing concerns with their EHRs, aka "gag clauses".

Six months after publication

- Information blocking regulation goes into effect for all actors, including physicians. This also includes fee limitations on what EHR vendors can charge physicians related to access, use, and exchange of EHI.

Six to 24 months after publication

- EHI is limited to USCDI. Physicians and EHR vendors are required to support the access, use, and exchange of USCDI. If the full USCDI is not available, or if EHRs are not capable, information blocking exceptions can be used.
- Specific compliance requirements start for several EHR vendor conditions of certification, including fees charged for APIs, vendor transparency and product usability.
- "By no later than 24 months after publication," EHR vendors are required to update their certified EHR APIs to support FHIR capabilities and support the access, use, and exchange of USCDI.

24 months to 36 months and beyond

- 24 months post-publication and onward, all actors will be expected to be in compliance with the full definition of EHI, e.g., HIPAA-defined ePHI.
- By no later than 36 months after the rules' publication, EHR vendors must make it possible for physicians to extract the full definition of EHI (e.g., HIPAA-defined ePHI), using a certified EHI Export Capability. This supports physicians wanting to switch EHR products, patient accessing their full medical record, and population health analysis and reporting.