AMA
AMERICAN MEDICAL ASSOCIATION

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.

The AMA commented that HHS should reduce the complexity of its proposed information blocking regulation. In response to AMA concerns, HHS is postponing the enforcement of information blocking regulations on all actors for six months after the rule is officially published. 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 was overly broad.

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. HHS' finalized a glide path from the USCDI to ePHI which 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.*

<u>*Exceptions*</u>

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, if appropriate 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: The Preventing Harm Exception is intended to protect practices that the actor reasonably believes will substantially reduce the risk of patient harm or harm to another individual that would arise from the access, exchange or use of EHI, provided that the practice is no broader than necessary to substantially reduce the risk of harm and meets several conditions.

Privacy Exception: 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. An actor's conduct meets the Privacy Exception if it meets one of four separate sub-exceptions.

Security Exception: 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. Under the Security Exception, an actor's practice to protect the security of EHI is not information blocking if it is directly related to safeguarding the confidentiality, integrity and availability of EHI.

Fees Exception: 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.

Infeasibility Exception: 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.

Licensing Exception: 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.

Health IT Performance Exception: 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. These practices must last no longer than necessary.

Content and Manner Exception: 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."

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.

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

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.

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).

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 out 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.

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.

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

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."

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.

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 enhanced technical capabilities (e.g., the Fast Healthcare Interoperability Resources standard) 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.