hfma
healthcare financial management association

Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-facilitated Exchanges and Health Care Providers

March 9, 2020 Announcement of Final Rule
(CMS-9115-F)

On March 9, 2020, the Centers for Medicare & Medicaid Services (CMS) announced on its website a final rule on interoperability and patient access to health data. Under the final rule, Medicare Advantage (MA) plans, state Medicaid and Children's Health Insurance Program (CHIP) agencies, Medicaid and CHIP managed care plans, and qualified health plan (QHP) issuers in the federally-facilitated exchanges (FFEs) must meet certain requirements regarding patient access to their health care information, including requirements related to application programming interfaces (APIs).

The rule also finalizes requirements under the Conditions of Participation for hospitals to transmit electronic patient event notifications, requirements for public reporting related to provider attestations regarding information blocking, and updates requirements for states to exchange data regarding individuals dually eligible for Medicare and Medicaid.

Simultaneous with the announcement of this final rule, the Office of the National Coordinator for Health Information Technology (ONC) of the Department of Health and Human Services (HHS) announced a related final rule "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program," which implements certain provisions of the 21st Century Cures Act (P.L. 114-255), including those involving information blocking, conditions and maintenance of certification requirements for health information technology (health IT) developers, and modifications to ONC's 2015 Edition health IT certification criteria.

CMS has created an Interoperability and Patient Access final rule web page that includes links to implementation guidance and other materials relevant to this final rule: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index.

IMPORTANT: Because this rule has yet to be officially posted for public inspection by the *Federal Register,* it is not an official final rule. As a result, changes to effective dates and substantive policy could be made before the official release

Table of Contents

I. Background

In this final rule CMS aims to use its authority to advance the electronic exchange of patient health information and improve patient access to their health information. The agency says the key "touch points" of the rule are:

- Enabling patients to access health information electronically without special effort through APIs.
- Ensuring that providers have access to information on patients regardless of where they previously received care; preventing providers from inappropriately restricting the flow of information to other providers and payers; and reducing burden on providers.
- Ensuring that payers make enrollee electronic health information available through an API.
- Making it easy for patients and providers to identify providers within a plan's network.

The history of HHS efforts to promote interoperability of electronic health records was reviewed in the proposed rule (84 FR 7612-14). This includes provisions of the 2017 Executive Order 13813 to Promote Healthcare Choice and Competition Across the United States, the myHealthEData initiative, and a variety of other activities dating back to the 2004 creation of the ONC and the 2009 enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 115-5).

Challenges and barriers to interoperability are described, which CMS identified through stakeholder meetings, comments received on RFIs, through letters and during rulemaking. The major barriers named are the lack of a unique patient identifier (the subject of an RFI in the proposed rule); the lack of standardization; information blocking; the lack of adoption of certified health information technology among post-acute care providers; and privacy concerns.

II. Technical Standards Related to Interoperability

In this section of the rule CMS describes the framework and general approach it has taken in finalizing specific standards for MA organizations, state Medicaid and CHIP agencies, Medicaid and CHIP managed care organizations, and QHP issuers in the FFEs (referred to collectively in the preamble to the rule as "payers") that are set forth in section III.C, summarized below.

A. Technical Approach and Standards

For purposes of this final rule, CMS uses the definition of *interoperability* that appears in section 3000 of the Public Health Service Act (as amended by the 21st Century Cures Act):

> The term "interoperability", with respect to health information technology, means such health information technology that-
>
> (A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;
>
> (B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
>
> (C) does not constitute information blocking as defined in section 300jj–52(a) of [the Public Health Service (PHS) Act].

CMS states that a core policy principal in the final rule is that "...every American should be able, without special effort or advanced technical skills, to see, obtain, and use all electronically available information that is relevant to their health, care, and choices – of plans, providers, and special treatment options." The types of information envisioned are both specifically about the individual (which requires protection of the individual's privacy) and information of general interest that should be widely available (e.g., a health plan's provider network, formulary, and coverage policies).

An API is described as a set of commands, functions, protocols, or tools published by a software developer that enables other developers to create programs (applications or "apps") that interact with the software without needing to know its internal workings and that maintain consumer data privacy standards.

CMS is using its authority in Medicare, Medicaid, CHIP and over QHPs in FFEs to require that plans in these programs adopt and implement openly published, secure, standards-based APIs. These have been generally referred to as "open APIs" in the proposed rule and elsewhere, but CMS is concerned that the word open may suggest "not secure." Therefore, the term "standards-based API" is used in this final rule instead.

CMS intends that enrollees in these plans will be able to use an application (or "app") of their choice to access their own electronic health information and other information to manage their health. It believes that under the final rule claims and encounter information will become easily accessible for the vast majority of patients enrolled with payers regulated by CMS, and hopes that state-based exchanges may adopt similar standards for participating QHPs and that other payers will voluntarily offer enrollees the type of data access provided under this final rule.

As described further below, CMS is relying on the API technical standard adopted in the separately published ONC final rule on interoperability. However, CMS emphasizes that payers are not required to use ONC-certified Health IT Modules to make administrative data such as claims history or provider directory information available to enrollees.

Three key attributes of standards-based APIs are identified by CMS: standardized API technologies, technically transparent APIs, and APIs implemented in a pro-competitive manner. These features were discussed in detail in the proposed rule, and CMS says no comments were received on that general discussion.

B. Privacy and Security Concerns in the Context of APIs

CMS acknowledges stakeholder concerns about the privacy and security risks created by an API connecting to third-party applications. This was discussed in the proposed rule, where CMS noted that under the Health Insurance Portability and Accountability Act (HIPAA), covered entities and business associates responsible for protected health information (PHI) might believe they are responsible for determining whether an application to which an individual directs their PHI applies appropriate safeguards for the information it receives. At that time CMS reiterated and cited Office of Civil Rights (OCR) guidance[1] under which covered entities are not responsible for the security of PHI under HIPAA rules once PHI has been received by a third-party application chosen by an individual. Further, with respect to stakeholder concerns that unscrupulous actors could use direct-to-consumer applications to profit from obtaining and using or disclosing PHI without the individual's authorization, CMS noted that the Federal Trade Commission has the authority to investigate and take action against unfair trade practices. In order to ensure that enrollees are better informed about how to protect their PHI, in section III CMS finalizes requirements on payers to assist in this regard.

HIPAA-covered entities and business associates are encouraged to review their responsibilities under HIPAA considering the recent decision in *Ciox Health, LLC v. Azar, et al*., (No. 18-cv-0040; D.D.C. January 23, 2020)[2]. This ruling vacates a portion of the HIPAA Privacy Rule that provides an individual the right to direct a covered entity to send protected health information that is not in an EHR to a third party identified by the individual. CMS notes that this decision does not affect its programmatic authorities to finalize the standards-based API requirements for the programs specified in this rule, nor does it alter the rights of an individual under HIPAA to request and obtain a copy of their records. CMS believes that because the goal of the standards-based API requirement is to give patients access to their own information for their own personal use, the final rule policies are consistent with the spirit of access rights under HIPAA.

CMS responds to many comments regarding privacy and security of APIs. It emphasizes that once data are transmitted and no longer under the control of the HIPAA-covered entity or business associate, those entities no longer have any obligation under HIPAA for the privacy and security of the PHI, and these data are no longer subject to HIPAA. As discussed below, the only circumstance under which a payer can deny access to an app is if the payer (or business associate's) own systems would be endangered by engagement with the app through an API. Under HIPAA, payers are free to advise patients on the potential risks involved with transferring data to an app that is not covered by HIPAA, but the payer may not substitute its own judgment for the patient's and must share the data if the patient still wants the transfer after being provided

[1] Readers are referred to OCR guidance available at this link: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
[2] Court documents on this case available at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2018cv0040-51 and https://hds.sharecare.com/wp-content/uploads/2020/01/CiOX-Health-v.-HHS-Court-Order-3-24-2020.pdf

the information. As noted earlier, CMS finalizes requirements for payers to provide educational information to enrollees on protecting the security of their PHI (summarized in section III below).

As discussion in section III below, under this rule payers are required to education patients on how to choose a third-party app that best mitigates risks associated with secondary data uses. CMS will provide payers with suggested content for this purpose and a framework for requesting that third-party apps attest to addressing certain issues in their privacy policy, including informing users about secondary data use.

Some commenters suggested creating a safe harbor for HIPAA-covered entities when transferring data to an app. CMS says that it does not have authority to do this and it also does not believe this is necessary because covered entities and business associates are not responsible for the data once it has been transferred. Comments on overlapping federal and state privacy laws and the need for new consumer privacy protections are deemed beyond the scope of this regulation.

Agreeing with commenters that app developers are not subject to regulations protecting the privacy and security of electronic health information, CMS notes that although it cannot regulate third-party apps directly, it is sharing information with app developers on best practices and lessons learned from its experience with Blue Button 2.0. (See the web page link on page 1 of this summary.) In addition, the ONC final rule includes technical requirements for APIs that enable and support persistent user authentication and app authorization, although CMS recognizes that this does not address concerns about data security with the third party.

In the proposed rule, CMS requested comments on whether existing privacy and security standards, including those under HIPAA, are sufficient for its API policies or whether additional privacy and security standards should be required. In responding to comments it received regarding privacy and security around consent, authentication, and verification, CMS notes that the API security protocols it is adopting by reference to the newly finalized ONC API standard (45 CFR 170.215) include not only HL7 FHIR Release 4.0.1 but complementary security and app registration protocols, specifically the SMART Application Launch Implementation Guide 1.0.0, which is a profile of the OAuth 2.9 specification and the OpenID Connect Core 1.0 standard, incorporating errata set 1.[3] CMS says that this approach supports multifactor authentication, which it sees as a best practice for privacy and security in health care settings. In addition, this technology can be used to support parsing or segmenting data using the API, which HHS is exploring for the future.

Differences in terminology used in this final rule, the ONC final rule, and the OCR guidance are discussed in response to comments. CMS notes that OCR guidance refers to an “electronic health record system developer” and an “app developer” while this final rule refers to any “developer of

[3] Additional information on the SMART App Launch Framework is available at http://hl7.org/fhir/smart-app-launch/.

a third-party app," which may include an electronic record system developer. CMS notes that it does not use ONC program-specific terms in this rule.

C. Specific Technical Approach and Standards

The specific standards finalized for APIs and summarized in section III.C include content and vocabulary standards for representing electronic health information and technical standards by which an API must make electronic health information available. The standards align with the interoperability standards in the ONC final rule, and CMS notes that commenters agreed with this approach. The standards were detailed in the proposed rule and key elements are highlighted here.

- CMS finalizes its proposal to adopt by cross reference the API technical standard included in the ONC final rule (45 CFR 170.215). By doing this, it is effectively requiring the use of the foundational Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR) Release 4.0.1 standard with associated implementation specifications and OpenID Connect Core 1.0, incorporating errata set 1.
- The specific content and vocabulary standards finalized in this rule are:
  - United States Core Data for Interoperability (USCDI) Version 1[4], as adopted in the ONC final rule (45 CFR 170.213) and
  - HIPAA Administrative Simplification transaction standards (45 CFR part 162) or the Medicare Part D e-prescribing transaction standards (42 CFR 423.160) where required by law or where applicable to the data type or element

Payers may use updated versions of required standards if the updated version is required by another applicable law or is not prohibited under another law, provided that (1) for standards other than the USCDI, the Secretary has not prohibited use of the updated version, (2) for the USCDI and API standards, the ONC has approved updates to its standards for use in the ONC Health IT Certification program, and (3) use of the updated version does not disrupt an end-users ability to access data through the API.

III. Patient Access Through APIs

A. Background on Medicare Blue Button

CMS describes the Medicare Blue Button 2.0 initiative, under which beneficiaries can access claims and encounter data for Medicare parts A, B and D and share the information with apps, services and research programs through an API. CMS believes beneficiaries benefit from having secure access to claims data in a standardized computable format.

B. Expanding the Availability of Health Information

The benefits of information access are discussed. CMS views the combination of claims and encounter data used in conjunction with EHR data as providing a broader picture of an individual's interactions with the health care system than EHR data alone. It says these data can empower individuals to make informed health care decisions, and individuals can facilitate

[4] http://www.healthit.gov/USCDI

communication with multiple health care providers by allowing them to access the same information through a standards-based API. CMS notes that use of a standards-based API will provide an additional method for individuals to exercise the HIPAA right of access to PHI, although it may be that not all EHR information subject to the HIPAA right of access would be transferable through the API. For example, an X-ray image that is not captured in the USCDI would have to be shared in a manner other than the API.

C. Standards-based API for MA, Medicaid, CHIP, and QHP Issuers in FFEs

The specific requirements for payers to implement, test and maintain the standards-based API that permits third-party applications to retrieve data from the payer at the direction of an enrollee ("Patient Access API") are detailed in this section of the final rule. "Nearly identical" regulatory language is adopted for each payer; the sections of 42 CFR that are affected are those for MA organizations (422.119); state Medicaid fee-for-service programs (431.60); Medicaid managed care plans (438.242(b)); CHIP fee-for-service programs (457.730); and CHIP managed care plans (457.1233(d)). In addition, 45 CFR 156.221 is modified, which pertains to QHPs in FFEs. With respect to QHPs, the standards-based API requirement will not apply to issuers of stand-alone dental plans offered in FFEs, or to issuers of QHPs offered only in the Federally-facilitated Small Business Health Options Program Exchanges (FF-SHOPs). FFEs include those in states that perform plan management functions, but state-based exchanges on the federal platform (SBE-FPs) are not FFEs and therefore QHP issuers participating there are not subject to the requirements of this rule.

The regulations for each payer follow the same basic structure. In each section, paragraph (a) requires the entity to implement and maintain a standards-based API that permits third-party applications to retrieve, with the approval and direction of the individual, data specified in paragraph (b) through the use of common technologies and without special effort from the enrollee. "Common technologies" refers to smart phones, home computers, laptops or tablets and the like. The term "without special effort" reflects CMS' expectation that third-party software as well as proprietary applications and web portals operated by the payer could be used to connect to the API and provide the enrollee access to the data. Paragraph (c) identifies the API technical standard along with content and vocabulary, testing, and updating requirements; paragraph (d) the documentation requirements; paragraph (e) authority for the payer to deny or discontinue access to the API; paragraph (f) requirements for payer-to-payer data exchange; and paragraph (g) the requirements for posting information on security and privacy for beneficiaries. These requirements and others are described immediately below, except for paragraph (f) which is discussed in section IV. All requirements are generally effective January 1, 2021 unless otherwise noted.

Statutory Authority to Require Implementation of a Standards-based API. With respect to each payer, CMS describes the statutory authority under which it is promulgating the standards-based API requirements; that discussion is not detailed for purposes of this summary. While it does not have authority to apply the standards-based API requirements to QHPs solely in state-based exchanges (SBEs), CMS encourages SBEs to consider whether a similar requirement should apply to QHPs in these exchanges.

API Technical Standard; Content and Vocabulary Standards. As discussed earlier, the payers covered under this final rule are required to implement a standards-based API technology that conforms with the API technical standards adopted at 45 CFR 170.215 in the ONC final rule. In addition, the content and vocabulary standards at 45 CFR part 162 and 42 CFR 423.160 and in 45 CFR 170.213 must be met (see section II.C above). At the suggestion of some commenters, the final rule includes new regulatory text specifying that beginning January 1, 2021 (or for QHPs on the FFEs, plan years beginning on or after January 1, 2021), payers must make available the data they maintain with a service date on or after January 1, 2016. That is, no information with an earlier date of service will need to be provided through the Patient Access API. CMS believes that this date balances patient benefit with compliance cost and burden. In addition to the amendments to the regulatory sections listed above for each payer, conforming changes to other regulatory text are made. As discussed in section II.C, CMS finalizes that payers may use updated versions of required standards under certain circumstances. In addition, while a payer must use the required standards to provide the required information through the API, the final rule does not preclude a payer from including additional information that is not required using other available standards.

Responding to comments on the cost of compliance, CMS notes that compared with the proposed rule, the estimated first-year impact of the standard-based API in this final rule has been doubled to just under $1.6 million per payer. CMS further acknowledges that these costs may be passed on to patients in premiums, but notes that government primarily bears the cost for MA, Medicaid and CHIP enrollees as well as QHP enrollees who receive premium tax credits. (CMS outlines how for each type of payer the federal government will participate in covering the costs.) It believes the benefits of a Patient Access API outweigh the costs. CMS further believes that the revised estimated impact is ‘minimal’ relative to the scale of the payers involved.

Regarding concerns about implementation of APIs, CMS refers readers to the specific implementation guides available through the final rule web page (final rule web page link provided on page 1 of this summary.)

Some comments addressed the need for payer contracts with providers to specify the timing of provider supply of the data that must be available through the API. CMS does not believe that it should require standardized contracts for this purpose, however, as it believes that payer-provider relationships are unique. CMS believes the implementation dates in the final rule will allow enough time to address these issues.

Data Required to be Available Through Standards-based API; Timeframes for Data Availability. CMS finalizes that, at a minimum, the information listed below must be made available through the API. The specific data requirements vary for each payer but generally include the following:

- adjudicated claims data, including provider remittances and enrollee cost sharing
- encounters with capitated providers
- clinical data, including laboratory results (but only if managed by the payer);
- formulary information (for MA-PD plans) or information about covered outpatient drugs and preferred drug lists (for state Medicaid and CHIP agencies, Medicaid managed care plans and CHIP managed care entities).

CMS does not finalize its proposals to include provider directory and pharmacy directory data in the Patient Access API because this information is required in the Provider Directory API, discussed below.

The requirements represent the minimum content that must be shared through the Patient Access API; CMS encourages payers to make additional data available.

Adjudicated claims data includes data on approved and denied claims, and that for which the plan has made an initial payment decision even when the period during which an enrollee can file an appeal is still in effect, or when the enrollee has filed an appeal and is awaiting a reconsideration decision. CMS notes that under the final rule payers are not required to conduct any additional review or audit of claims for purposes of this requirement beyond current practices. A payer may include a disclaimer or other notice as part of the API to indicate this.

Responding to comments indicating that claims data are not useful to enrollees, CMS responds that these data provide information to enrollees on the names of providers they visited, dates of visits, dates and other information on tests and procedures, all of which can be useful to patients in planning care with their providers.

With respect to comments concerned with disclosure of a payer's negotiated rates, CMS says that these data are already available to patients and there is broad value in patients better understanding the costs of their health care services. While CMS acknowledges that an app could potentially aggregate data across patients and use that information in other ways than what is intended in this rule, it does not have the authority to regulate third-party apps.

The time requirements within which the required information must be made available to the API vary by payer, as shown in the following table, and are unchanged from the proposed rule.

	MA	**Medicaid and CHIP**	**QHP in FFE**
Regulatory text	42 CFR 422.119(b)	42 CFR 431.60(b) and 457.730(b)	45 CFR 156.221(b)
Claims data	1 business day after processed	1 business day after processed	1 business day after processed
Encounter data	1 business day after receipt	1 business day after receipt*	1 business day after receipt
Clinical data including lab results, if maintained by the payer	1 business day after receipt	1 business day after receipt	1 business day after receipt
Formulary (or for Medicaid and CHIP FFS, info on covered outpatient drugs)	Unspecified**	1 business day after updates effective	N/A

*States are not required to provide encounter data received from managed care plans through the API. Separate requirements for Medicaid and CHIP managed care plans to provide encounter data through an API appear at 438.242(b)(5) and 457.1233(d)(2).

**CMS intends that the Part D requirements in 42 CFR Part 423 regarding the timing of pharmacy directories would apply to provision of this information through the API.

Some commenters were concerned with the 1-day deadlines and suggested various ways in which the final rule could provide for more time, but CMS responds that providing timely data to enrollees is important. CMS also emphasizes that the requirement is for 1 business day after the claim is adjudicated or encounter data are received, which allows for potential delays in adjudication or delays in providers submitting their encounter data. Analysis of Chronic Conditions Data Warehouse data indicates that nearly half of all Medicare FFS or carrier claims are submitted once and unchanged, nearly 85 percent of inpatient claims are never adjusted, and 99 percent of carrier claims are fully mature at 10 months. CMS concludes that because many claims remain unchanged, and those that do take more that 3 or 5 days after adjudication to begin to mature, providing a few days additional time for payers to make the data available to the API would not provide enrollees with more accurate or complete data.

CMS states that payers and providers are not required to change their contractual relationships or current processes under this requirement, although it strongly encourages them to work together to make patient data available in as timely a manner as possible. Modifying payer/provider contracts is one approach. CMS believes that providers can benefit from making this information available sooner, as it could result in more timely care coordination. However, it notes that establishing any timeframes beyond the one in the final rule (information available to patients via the Patient Access API within one (1) business day after the payer receives the information) is a matter between the payers and their providers.

Under the finalized clinical data requirement, any clinical data included in the USCDI Version 1, as adopted in the ONC final rule (45 CFR 170.213), must be made available through the API if the data is received and maintained by the payer as part of its normal operations. The regulatory text is changed from the proposed rule to eliminate reference to a payer that "manages" the data in favor of "maintains." Clinical data include laboratory tests and must be provided through the Patient Access API regardless of how the data were received by the payer, except that data received through the payer-to-payer exchange finalized in this rule (section IV below) must only be provided through the API if they were received through a standards-based API. CMS intends to work with HL7 and others to provide implementation assistance to payers; readers are referred to the implementation guidance (link on page 1 of this summary).

In responding to comments, CMS agrees that payers are not typically the original source of clinical data, but because payers maintain these data which are of value to patients, they should be available through the API. CMS notes that data provenance is one element of the USCDI and will be available to patients. Further, payers can indicate which data come from outside sources so that patients can appropriately direct questions. Suggested content for patient educational materials will be provided. With respect to sensitive patient data, CMS reminds readers that data are exchanged via the API at the approval and direction of the patient; providers remain subject to HIPAA requirements.

Documentation Requirements for APIs. CMS finalizes that regulated payers are required to publish complete documentation regarding the API on their website or via a publicly accessible hyperlink. To address commenter questions, the final regulatory text is modified to clarify that publicly accessible means that any person using commonly available technology to browse the internet could access the information without any preconditions or additional steps such as collecting a fee to access the documentation, requiring the reader to receive a copy via email, requiring the user to register or create an account, or requiring the user to read promotional material or agree to receive future communications from the organization making the documentation available.

The publicly accessible documentation must include, at a minimum, the following:

- API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
- The software components and configurations an application must use in order to successfully interact with the API (for example, to connect and receive data through the API) and process its response(s).
- All applicable technical requirements and attributes necessary for an application to be registered with any authorization server(s) deployed in conjunction with the API.

Routine Testing and Monitoring of Standards-based APIs. The API must be routinely tested and monitored to ensure it is functioning properly, including assessments to verify that it is fully and successfully implementing privacy and security features, such as HIPAA requirements. CMS adds language to the proposed rule regulatory text to specify that the API must be updated as appropriate to ensure it functions properly and verifies that an individual enrollee or their personal representative can only access PHI belonging to that enrollee. The final regulatory text is further modified to remove the word "minimally" with respect to compliance with privacy and security features. CMS intends to provide best practice information on testing.

Issues Related to Denial or Discontinuation of Access to the API. The final rule specifies the circumstances under which the regulated payers, which are all HIPAA-covered entities, may decline to establish or may terminate a third-party application's connection to their API while remaining in compliance with the standards-based API requirements.[5] CMS notes that the circumstances apply to specific applications and not the third party itself; the issue is the risk to the security of the payer's systems and not the type of data being exchanged (i.e., whether or not it is PHI). In response to comments requesting more clarity, changes are made to the regulatory text from the proposed rule to specify that the determination is made consistent with a security risk analysis under 45 CFR part 164 subpart C. In addition, after reflecting on commenter concerns and suggestions, CMS goes beyond the proposed rule and provides an option under which a payer may ask a third-party app to attest to certain privacy provisions and help make patients aware of privacy risks. Recognizing that although it does not have authority to regulate

[5] Under OCR guidance, when an individual asks to receive their data under the HIPAA Right of Access, covered entities must comply, including having to transmit data to a third party. Disagreement with the requesting individual about the worthiness of the third-party recipient of PHI or concerns about what that third party might do with PHI are not grounds for denying a request. However, a covered entity is not expected to tolerate unacceptable risk to its own systems as determined by its own risk analysis. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

third party apps, CMS takes this step to address the strong support of stakeholders for more privacy and security measures.

Specifically, under the final rule a payer regulated by this final rule may deny or discontinue any third-party application's connection to the standards-based API if it:

- Reasonably determines, consistent with its security risk analysis under 45 CFR part 164 subpart C, that allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of protected health information on the organization's systems; and
- Makes this determination using objective, verifiable criteria that are applied fairly and consistently across all applications and developers through which enrollees seek to access their electronic health information, including criteria that may rely on automated monitoring and risk mitigation tools.

Where access has been denied, CMS encourages payers and third-party apps to work together to address the concerns. While CMS says it does not have the authority to put a time frame on this process, it notes that the HIPAA Privacy Rule requires that information be provided in a timely manner.

Under the optional attestation policy, a payer covered under this final rule is encouraged to request, before giving access to its API, that third party apps attest to having certain provisions included in their privacy policies. CMS notes that if an app has a written privacy policy and does not follow its policies as written, the Federal Trade Commission (FTC) has authority to intervene. CMS suggests that attestation state that the app attest to the following:

- Having a publicly available privacy policy, written in plain language, that has been affirmatively shared with the patient (e.g., through a click or box check) prior to the patient authorizing app access to their health information.
- The privacy policy includes, at a minimum, the following information:
    - How a patient's health information may be accessed, exchanged, or used by any person or other entity, including whether the patient's health information may be shared or sold at any time (including in the future);
    - A requirement for express consent from a patient before the patient's health information is accessed, exchanged, or used, including receiving express consent before a patient's health information is shared or sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction);
    - If an app will access any other information from a patient's device; or
    - How a patient can discontinue app access to their data and what the app's policy and process is for disposing of a patient's data once the patient has withdrawn consent.

CMS suggests that payers look to the CARIN Alliance's Code of Conduct and the ONC Model Privacy Notice and other industry best practices for other provisions to include in their attestation request. Payers requesting an attestation may not discriminate in its implementation, including for the purposes of competitive advantage.

If the third-party app does not attest to having a privacy policy that meets the specified conditions, the payer may notify patients and advise them to reconsider using the app. The patient notification should explain the conditions to which the third-party app did not attest, and that the patient should use caution before opting to disclose information to the app. However, if after this notification the patient still requests the payer to make their data available to the app, the payer must comply unless the app is determined to endanger the security of PHI on the payer’s systems. CMS states that this process should not overly delay the patient’s access; that the payer should quickly inform the patient if the app fails to attest and provide a short window for the patient to cancel their request for data sharing. In the absence of a response from the patient, the payer must proceed to honor the initial request for data sharing with the third-party app.

CMS believes that the attestation, combined with the requirement for payers to provide patients with educational resources about privacy and security (described next) will better inform patients and help create a safer data exchange environment. Suggestions from some commenters that CMS adopt a certification or vetting process for third party apps are rejected. Although CMS appreciates that payers and providers are interested in vetting, it believes that the industry is in the best position to identify which apps have strong privacy and security features, and it does not have the authority to require third party apps to participate in a certification program.

Enrollee and Beneficiary Resources Regarding Privacy and Security. Payers regulated by this rule are required to make available to current and former enrollees certain information related to privacy and security of PHI. Each payer is required to provide educational resources in an accessible location on its public website and through other normal communication channels with current and former enrollees seeking to access their health information held by the payer. This could include customer portals, online customer service, and other locations.

At a minimum the resources must explain in non-technical, simple and easy-to-understand language:

- General information on steps the individual may consider taking to help protect the privacy and security of their health information, including factors to consider in selecting an application including secondary uses of data, and the importance of understanding the security and privacy practices of any application to which they will entrust their health information; and
- An overview of which types of organizations or individuals are and are not likely to be HIPAA covered entities, the oversight responsibilities of OCR and FTC, and how to submit a complaint to OCR or FTC.

In the proposed rule, CMS indicated that organizations could meet this requirement by using materials available on the HHS or FTC websites that are designed for consumer audiences. An organization choosing to use its own materials would be responsible for ensuring the information remains current if laws and policies change over time.

However, responding to commenters suggesting that CMS should take responsibility for consumer education, CMS commits in this final rule to providing suggested content which payers can then tailor to their patient population. This content will be provided through normal communication channels and made available through the final rule web page (link on page 1 of this summary).

The regulatory text is modified from the proposed rule to add language specifying that payers must include a discussion about a third-party app's secondary uses of data when providing factors to consider in selecting an application. Another modification is to state the payer must make these materials available in an easily accessible location on its public website.

Exception or Provisions Specific to Certain Programs or Sub-Programs. CMS reviews provisions in the final rule that are unique to certain types of plans. Specifically, this involves the exclusion of stand-alone dental plans from the requirements for QHPs in FFEs as described earlier, and provisions specific to Part D (e.g., accessibility of Part D claims data) that would apply to MA-PD plans and not to other MA plans.

In addition, the final rule provides that an FFE may grant exceptions from the standards-based API requirements for plans applying for QHP certification if the FFE determines it is in the best interests of the qualified individuals and employers where it operates. To receive an exception a plan applying for QHP certification would have to provide a narrative justification describing the reasons why it cannot reasonably satisfy the requirements, the impact of non-compliance upon enrollees, the current or proposed means of providing health information to enrollees, and solutions and a timeline to achieve compliance. CMS expects that these exceptions will be provided in limited circumstances such as small issuers, issuers who are only in the individual or small group market, financially vulnerable issuers, or new market entrants demonstrating that implementing a standards-based API would be a barrier to their ability to provide coverage to consumers and where not certifying the QHP would limit plan options for consumers.

In a change from the proposed rule, this exception would apply to a QHP that cannot meet *any* of the standards-based API requirements. The proposed rule would have applied the exception to a QHP that cannot meet the requirements to pertaining to retrieving the specified data and meeting the technical standard, along with the content and vocabulary, testing, and updating requirements.

In another change, the final rule adds that the standards-based API requirement does not apply to issuers of QHPs offered only in the Federally-facilitated Small Business Health Options Program Exchanges (FF-SHOPs). CMS believes that if this requirement applied it could reduce the availability of plans in the FF-SHOPs. In addition, it believes that most of these issuers would qualify for the exceptions otherwise provided in the final rule.

Applicability/Effective Dates. The effective date of the standards-based API requirements is January 1, 2021 for all payers, except for QHP issuers in FFEs, for which the API requirements would be effective for plan years beginning on or after January 1, 2021. CMS encourages payer to implement the policies as soon as possible. States are reminded that if they determine that because of these requirements a retroactive adjustment to capitation rates for Medicaid or CHIP managed care plans is warranted, they must have an actuarial certification and submit a revised rate certification with CMS as a contract amendment.

Information Sharing Between Payers and Providers through APIs: Request for Information. CMS anticipates that in the future payers and providers may seek to coordinate care and share information on an overlapping patient population in a single transaction. This could facilitate better understanding of where patients are receiving care to better manage their care. While in some places regional health information exchange might coordinate such transmissions, direct provider-to provider or plan-to-plan exchange through existing trusted networks of beneficiary-facing third-party applications might be more appropriate elsewhere. The proposed rule sought comments on the feasibility of providers to request a download on a shared patient population, and whether this would leverage standards-based APIs. CMS will consider the comments it received for future rulemaking.

This section of the final rule CMS responds to a variety of comments and inquiries on the standards-based API requirement not addressed earlier.

D. Impact Analysis

In the collection of information requirements section of the final rule, CMS estimates that implementing the API requirements will result in an aggregate first year cost between $272 million and $816 million across 345 affected payers. ($788,414 to $2,365,243 per organization or state). In addition, estimated maintenance totals $54 million for activities such as testing, upgrades and vetting of third-party applications ($157,657 per organization or state). Considering information provided by commenters, the first-year implementation estimates are changed from the proposed rule; at that time CMS estimated costs at $275 million, the low end of the range they now provide.

IV. API Access to Published Provider Directory Data

This section of the final rule describes requirements for the "Provider Directory API". Prior regulations require the payers regulated under this rule must make their provider directory available on a website or, in the case of QHPs in FFEs, publicly accessible in addition to distribution and access for enrollees. However, CMS believes that also making the information available through an API could support development of applications that would pull in current information about available providers to meet the needs of enrollees. For example, a referring provider could use the up-to-date contact information obtained from the API directory to securely send patient information to the receiving provider. CMS believes provider burden will be reduced by allowing payers to share more widely the information about providers in their network and whether or not they are accepting new patients.

As noted above, CMS had proposed that what they are now calling the Patient Access API also include provider directory information, but they did not finalize that requirement to reduce confusion and limit duplication.

Under the final rule, payers must implement and maintain a publicly accessible standards-based API that maintains a complete and accurate directory of contracted providers that is updated at least 30 days after the payer receives provider directory information or updates to it. The information must include names, addresses, phone numbers and specialties. For MA organization that offer Part D prescription drug benefits, a pharmacy directory must also be provided to include name, address phone number, number of pharmacies in the network, and mix of pharmacies (e.g., retail). As noted earlier, CMS exempts QHPs in FFEs from this requirement because current regulations already require them to make provider directory information available in machine-readable format.

The API must conform with same technical and documentation requirements specified for the Provider Access API and described above (and, for example, set forth in 422.199(c) and (d) with respect to MA plans.) except for user authentication and other protocols that restrict availability of the information. It must be accessible through a public-facing endpoint on the payer's website. The regulations are found at 42 CFR 422.120(b), 431.70(b), 438.242(b)(6), 457.760(b), and 457.1233(d)(3) for MA plans, state Medicaid programs, Medicaid managed care plans, CHIP programs, and CHP managed care plans respectively.

As noted above, HL7 FHIR Release 4.0.1 is the technical API standards adopted in the ONC final rule (170.215). Additional implementation guidance will be provided on how to use the standard for the purpose of making the provider directory information available through the API. The final rule web page has a link to this information.

Responding to comments, CMS does not believe that it is appropriate to require real-time updates to provider directories because it is not operationally feasible for payers to do so currently. It notes that the 30-day requirement is a minimum and that payers may make the information available via the API on a shorter time frame. Similarly, CMS limited the required information to minimize burden but encourages payers to provide additional information to benefit enrollees.

V. Health Information Exchange and Care Coordination Across Payers: Establishing a Coordination of Care Transaction to Communication Between Plans

CMS finalizes, with some changes from the proposed rule, that MA organizations, Medicaid and CHIP managed care plans and QHPs in FFEs must maintain a process for the electronic exchange of the data classes and elements included in the USCDI Version 1 data set standard adopted in the ONC final rule (45 CFR 170.213) and described in section II.C above. Under this payer-to-payer data exchange, with the approval and at direction of a current or former enrollee (or their representative), a payer must receive this information from another payer that had covered the enrollee within the preceding 5 years and incorporate it into its records about the enrollee. In addition, for current enrollees and for up to 5 years after disenrollment, a payer must send data to any other payer that currently covers the enrollee or to which the enrollee specifically requests the data be provided.

When a payer is sending data to another payer, data it previously received from another payer is to be sent in the electronic form and format in which it was received. CMS makes this change from the proposed rule in order to minimize burden on payers; a payer is not required to receive or share paper records from another payer under this provision.

The requirement for payer-to-payer data exchange of USCDI data is effective January 1, 2022; for QHPs in the FFE, it is for plan years beginning on or after January 1, 2022). The requirement is limited to data with a service date on or after January 1, 2016. CMS believes that this effective date provides enough time for payers to meet the Patient Access API requirements and implement payer-to-payer data exchange.

The regulatory text for this requirement appears at 42 CFR 119(f) for MA organizations; 438.62(b)(1)(vi) for Medicaid managed care plans (and cross referenced for CHIP managed care entities); and at 45 CFR 156.221(f) for QHPs in the FFEs.

CMS believes that use of the USCDI to exchange information furthers care coordination. Examples offered are reducing the need for health care providers to write letters of medical necessity; reducing instances of inappropriate step therapy; reducing repeated utilization reviews, risk screenings and assessments; streamlining prior authorization processes; and reducing instances where health care provider needs to intervene with a plan to ensure a patient receives needed treatment. These are all areas which CMS says stakeholders have previously raised as examples of administrative burdens.

In addition, by providing access to multiple years of their health care information, CMS believes patients will have a more comprehensive history of their medical care. The USCDI data set includes laboratory and other test results, medications, health concerns, clinical notes, assessments and treatment plans and other data points needed for care coordination.

The final rule allows for multiple methods for electronic exchange of information, not limited to the standards-based API; CMS is considering future rulemaking to require an API-based payer-to-payer data exchange.

In the regulatory impact analysis section of the final rule, CMS estimates that its policies will have minimal costs on plans. It says it is difficult to quantity the impact because the methods that plans will use to share information (e.g., APIs, health information exchanges) cannot be predicted.

VI. Care Coordination Through Trusted Exchange Networks: Trusted Exchange Network Requirements for MA Plans, Medicaid Managed Care Plans, CHIP Managed Care Entities, and QHPs in the FFEs

CMS does not finalize its proposal that the payers regulated under this final rule must participate in trusted exchange networks in order to improve interoperability. Although it believes in the positive role that trusted exchange networks can play, it agrees with commenters that the true value of this concept might best be realized in the future when the Trusted Exchange Framework and Common Agreement (TEFCA) has matured.

VII. Improving the Medicare-Medicaid Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges

CMS finalizes without changes its proposals to increase the frequency of federal-state data exchanges for individuals dually eligible for Medicare and Medicaid. It believes that the interoperability of CMS eligibility systems is critical to modernizing the programs and improving the experiences of beneficiaries and providers, and sees increasing the frequency of data exchanges as a strong first step.

A. State Buy-in for Medicare Parts A and B

Currently, all states and the District of Columbia have agreements with CMS to facilitate state “buy-in” of the Medicare Part B premium on behalf of dual eligibles; 36 states and DC have a buy-in agreement for Part A premiums. Data is submitted by the state via an electronic file transfer (EFT) exchange setup; CMS responds and may push updates from the Social Security Administration such as a change in the beneficiary identification number or address.

Current guidance provides that states should exchange buy-in data at least monthly, with the option for daily or weekly exchange. States may also choose how frequently to receive the CMS response data file. CMS reports that 25 states and DC are submitting buy-in data to CMS daily and 32 states and DC are receiving response files from CMS daily. CMS is concerned that in states that exchange data monthly the lag in updating buy-in data means that the state or beneficiary may be paying premiums for longer than appropriate. Recoupment and redistribution of funds is a burdensome administrative process between the beneficiary, state, CMS, and SSA. It can take multiple months to correct and resubmit an improperly processed transaction, exacerbating the delays in appropriately assigning premium liability.

Therefore, CMS finalizes a change to existing regulations to require that all states participate in daily exchange of buy-in data to CMS (meaning every business day for which a new transaction is available to transmit). The change will be effective April 1, 2022; CMS believes this will provide the affected states (26 submitting buy-in data and 19 for receiving it) with enough time to phase in operational changes or bundle this requirement with other systems updates. In the regulatory impact analysis section CMS states that the one-time cost to a state will be $85,000 per change (i.e., $170,000 for a state that needs to change make changes for both sending and receiving data daily), and the aggregate cost to states of implementing this requirement would be $3.9 million.

B. Exchange of MMA Data Files

Under the Medicare Modernization Act (MMA) (P.L. 108-173) primary responsibility for prescription drug coverage for full-benefit dual eligibles shifted to the Medicare program. Implementing regulations (42 CFR 423.910) require states to report at least monthly a file identifying full-benefit and partial-benefit dually eligible beneficiaries in the state. This has come to be called the “MMA file” or “State Phasedown File.” In addition to information exchange related to Part D, these data are used to support risk adjustment of MA plans, and to inform Part A and B eligibility and claim processing systems so that providers, suppliers and beneficiaries have accurate information on beneficiary cost-sharing obligations.

Most states submit the MMA data files at least weekly; only 13 states do so daily. Because dual eligibility status can change at any time, CMS believes that monthly status updates prevent access to the correct level of benefit at the correct level of payment. While it has instituted work-arounds, CMS believes more frequent data exchange would be preferred. Advantages of daily data exchange that CMS sees include enabling an earlier transition to Medicare coverage for prescription drugs; reducing claims paid erroneously by the state; effectuating an earlier shift to Medicare as primary payer for many services; aiding timely error identification and resolution; supporting states that promote enrollment in integrated care such as Dual-eligible Special Needs Plans, Medicare-Medicaid Plans, and the Programs for All-inclusive Care for the Elderly (PACE) by expediting the enrollment into Medicare; supporting earlier beneficiary access to Medicare Part D benefits and related subsidies sooner; and promoting protections for qualified Medicare beneficiaries (QMBs) by improving the accuracy of data for providers and QMBs on zero cost-sharing liability for services under Medicare Parts A and B.

Therefore, CMS finalizes an update to the frequency requirements (in 42 CFR 423.910(d) and conforming changes) to require that starting April 1, 2022, all states submit the required MMA file data to CMS daily (every business day for which a new transaction is available to transmit). CMS believes this effective date will provide states with enough time to make operational changes or bundle this required change with any new systems implementation. CMS estimates the aggregate cost of this provision to be $3.1 million.

VIII. Information Blocking Background and Public Reporting

CMS reviews activities regarding information blocking. In 2015 ONC issued the Information Blocking Congressional Report, which concluded that information blocking is a serious problem and that the Congress should prohibit it and provide penalties and enforcement mechanisms to deter these practices. At the same time, the Congress enacted the Medicare Access and CHIP Reauthorization Act (MACRA), which requires that for purposes of demonstrating meaningful use of CEHRT, an eligible professional must demonstrate that he or she has not knowingly and willfully taken action (such as to disable functionality) to limit or restrict the compatibility or interoperability of CEHRT. MACRA imposed similar requirements on hospitals and critical access hospitals (CAHs). To implement these information blocking prevention provisions, CMS adopted attestation requirements, consisting of three statements about a provider's use of CEHRT[6]. To satisfy the Promoting Interoperability performance category of the Quality Payment Program (QPP) or, in the case of hospitals and CAHs, to meet the requirements of the Promoting Interoperability Program, a provider must attest "yes" to each of the statements.

A recent survey of health information organizations is cited, which found that half reported that EHR developers routinely engage in information blocking, and that one quarter reported that hospitals and health systems routinely do so.[7] Strengthening competitive position is seen as a motivation, but CMS says other research finds that these practices limit patient mobility, encourage consolidation and create barriers to entry for innovation.

The Cures Act added an information blocking provision (section 3022) to the PHS Act. It defines information blocking and creates possible penalties and disincentives to these practices. It

[6] The attestation requirement at 42 CFR 1375(b)(3)(ii) follows: *Support for health information exchange and the prevention of information blocking.* The MIPS eligible clinician must attest to CMS that he or she—(A) Did not knowingly and willfully take action (such as to disable functionality) to limit or restrict the compatibility or interoperability of certified EHR technology. (B) Implemented technologies, standards, policies, practices, and agreements reasonably calculated to ensure, to the greatest extent practicable and permitted by law, that the certified EHR technology was, at all relevant times—(*1*) Connected in accordance with applicable law; (*2*) Compliant with all standards applicable to the exchange of information, including the standards, implementation specifications, and certification criteria adopted at 45 CFR part 170; (*3*) Implemented in a manner that allowed for timely access by patients to their electronic health information; and (*4*) Implemented in a manner that allowed for the timely, secure, and trusted bi-directional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate certified EHR technology and health IT vendors. (C) Responded in good faith and in a timely manner to requests to retrieve or exchange electronic health information, including from patients, health care providers (as defined by 42 U.S.C. 300jj(3)), and other persons, regardless of the requestor's affiliation or technology vendor. Parallel language for hospitals and CAHs appears at 42 CFR 495.40(b)(2)(i)(I)(1) through (3).

[7] Julia Adler-Milstein and Eric Pfeifer, Information Blocking: Is It Occurring And What Policy Strategies Can Address It?, 95 Milbank Quarterly 117, 124–25 (Mar. 2017), available at http://onlinelibrary.wiley.com/doi/10.1111/1468-0009.12247/full

requires the Secretary to identify through rulemaking reasonable and necessary activities that do not constitute information blocking. The ONC final rule implements this provision.

In this rule, CMS finalizes without change its proposal to publicly report information on eligible clinicians' attestations under the QPP on the Physician Compare website, and to report similar information on attestations of hospitals and CAHs under the Medicare Promoting Interoperability Program on a CMS public website. In the 2018 QPP final rule (85 FR 53827) CMS adopted a policy to include an indicator (as technically feasible) for any eligible clinician or group who successfully meets the Promoting Interoperability performance category and to include additional information on profile pages or in the downloadable data base on objectives, measures and activities with respect to this performance category.

Specifically, under this final rule an indicator will be added on Physician Compare for eligible clinicians and groups that submit a "no" response to any of the three attestation statements. If a "no" response is submitted the attestations would be considered incomplete and no indicator would appear. The indicator will be posted on the profile pages or the downloadable data base as feasible and appropriate, beginning with the 2019 performance period data available in late 2020. All public reported data are available for review and correction under the QPP targeted review process. CMS intends to determine the best display and wording after testing and sharing with stakeholders through the Physician Compare Initiative page and other communication channels. It reiterates that the policy is contingent on the technical feasibility of using these data for public reporting.

Similarly, CMS will post information on a public website indicating any hospitals and CAHs that submit a "no" response to any of the three attestation statements. Information that is left blank will be considered incomplete and no information posted. The information will be posted beginning with the 2019 reporting period in late 2020. Hospitals and CAHs will have a 30-day preview period to review this information before it is publicly posted. During that time CMS will consider making changes on a case-by-case basis.

IX. Provider Digital Contact Information

The Cures Act (section 4003) requires the Secretary to create a provider digital contact information index. To meet this requirement CMS has updated the National Plan and Provider Enumeration System (NPPES) to capture digital contact information for individuals and facilities. The NPPES supplies National Provider Identifier numbers to providers, maintains the NPI record and makes the information available online.[8] Since June 2018 the NPPES has been updated to capture one or more pieces of digital contact information. This includes a Direct address and the ability to capture other endpoints for secure information exchange such as a FHIR server URL or query endpoint associated with a health information exchange. Each provider can maintain unique information or associated themselves with information shared among a group of providers. NPPES has also added a public API which can be used to obtain contact information stored in the database.

Because many providers have not yet submitted digital contact information and what is there is frequently out of date, CMS finalizes its proposal to publicly report the names and NPIs of

[8] See https://nppes.cms.hhs.gov/.

providers who do not have digital contact information stored in the NPPES beginning in the second half of 2020. Additionally, CMS will engage in public education efforts to ensure that providers are aware of the benefits of including digital contact information in the NPPES, and the public reporting policy

Providers can review their information using the NPPES NPI Registry (https://npiregistry.cms.hhs.gov/), the NPPES NPI Registry API (https://npiregistry.cms.hhs.gov/registry/help-api), or the NPPES Data Dissemination file (https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/NationalProvIdentStand/DataDissemination).

X. Revisions to the Conditions of Participation for Hospitals and Critical Access Hospitals (CAHs)

CMS discusses responses to the RFI on interoperability that it published in a number of proposed rules which requested input on how conditions of participation (CoPs) and similar CMS health and safety standards could be used to further advance electronic exchange of information; the discharge planning CoP rule (84 FR 51836) that was finalized on September 30, 2019, after the CMS proposed rule on interoperability was released is also discussed. The discharge planning rule requires that a patient's medical information be transferred with the patient after discharge from a hospital, CAH or post-acute care services provider. The discharge planning final rule also provides a patient right to access their medical records in an electronic format if the patient requests it and the hospital has the capacity to do so.

In this rule, CMS finalizes, with changes from the proposed rule, addition of a new electronic notification standard in the medical record services CoP for hospitals (§482.24(d)(2), psychiatric hospitals (§482.61(f)) and CAHs (§485.638(d)), effective 6 months after publication of this final rule. The new patient event notifications[9] standard applies to providers that have an electronic system that conforms to the HL7 2.5.1 content exchange standard, which is referenced at 45 CFR 170.205(d)(2). If so, they must demonstrate that the system's notification capacity is fully operational and that they use it in accordance with all state and federal statutes and regulations applicable to the hospital's exchange of patient health information.

To the extent allowed under federal and state laws and regulations, and consistent with a patient's expressed privacy preferences, a hospital must demonstrate that its system sends patient event notifications in the case of a patient's registration in the emergency department (ED), admission as an inpatient (regardless of the source of admission), discharge or transfer from the ED, and discharge or transfer from inpatient services, whichever are applicable to a patient. Notifications may be made directly or through an intermediary that facilitates exchange of health information (e.g., a health information exchange.) A reasonable effort is to be made to ensure notification of specified providers which need to receive notification of the patient's status for treatment, care coordination, or quality improvement purposes. The specified providers are all

[9] Patient event notifications are automated electronic communications from a discharging provider to another facility or to another community provider identified by the patient. CMS states that virtually all EHR systems generate these messages using admission, discharge and transfer (ADT) messages, a standard message used within an EHR to communicate changes in patient status as they are tracked by the system.

applicable post-acute services providers and suppliers; the patient's established primary care practitioner, group or entity; or other established practitioner, group or entity identified by the patient as primarily responsible for the patient's care. The notification must include at least the patient's name, treating practitioner name, and the name of the sending hospital.

The requirement for notification of ED registration was not in the proposed rule, which focused only on inpatient admissions, and is made in response to commenters. CMS agrees that ED notification provides an additional opportunity to improve continuity of care and patient care transitions. CMS describes several scenarios to illustrate when the notification would and would not be required; notification is generally tied to a change from outpatient to inpatient status. It says a patient registered in the ED (or as an observational stay) who is later admitted as an inpatient would require separate notifications for each event (i.e., ED registration and inpatient admission) whereas a patient admitted as an inpatient who is transferred between inpatient units (e.g., intensive care to a medical unit) would not require separate notices, although a hospital might choose to provide these.

Another change from the proposed rule is the elimination of the term "established care relationship" with respect to which providers are to receive the patient event notification. The final language narrows the recipients as the patient's established primary care practitioner, group or entity or another established practitioner, group or entity identified by the patient as primarily responsible for their care. CMS clarifies that where a patient has not identified a primary care practitioner, the hospital is not expected to provide such a notification. With respect to PAC providers, CMS indicates that the required recipients are those PAC providers with whom the patient had an established relationship immediately before admission or to which the patient is being transferred or referred at discharge. CMS believes these changes will relieve the potential provider burden from the language in the proposed rule. Other changes are made to the wording and structure of the regulatory text.

In responding to comments, CMS emphasizes that changes to the regulatory text in the final rule require only that a hospital "has made a reasonable effort" to ensure that its system sends the notifications to the specified providers. This is in lieu of language in the proposed rule that required notifications to be sent to providers for whom the hospital had a "reasonable certainty of receipt of notifications". CMS believes this change better reflects actions within the hospital's control and recognizes that some intended recipients may not be able to receive notifications. It does not expect a hospital to demonstrate that its system be able to communicate with every possible provider. Compliance will be based on system capabilities. For example, if direct messaging is used to send notifications, the surveyor might be expected to review wither the hospital has a system for capturing direct addresses of patients' primary care practitioners.

Further, unlike commenters concerned that the lack of data exchange infrastructure will make compliance with this requirement costly, inefficient, and burdensome, CMS believes that the existing infrastructure is sufficient to provide substantial support for the requirement that hospitals make a reasonable effort to ensure its systems send the notifications. It notes that in many areas health information exchanges are currently supporting patient event notifications.

In addition, the final language is modified to provide that where consistent with other federal and state laws, a hospital may honor patient preferences to restrict delivery of the notification. At the same time patient consent is not required for a hospital to send a patient event notification.

The final language eliminates diagnosis from the information required in the patient event notification, although CMS emphasizes that this does not preclude hospitals from including other patient information, such as diagnosis. It is not finalized because CMS agrees with commenters that including this information could be unnecessarily burdensome and prevent hospitals from satisfying this CoP standard using basic information available in an ADT message.

CMS notes that some comments disagreed with the use of CoPs to advance the use of patient event notifications, arguing that putting hospital participation in Medicare at risk would be an excessive penalty for failure to meet the patient event notification requirement. CMS believes that CoPs are an appropriate tool for this purpose. It believes that patient event notification should be a fundamental feature of hospital medical record systems to promote patient safety and effective care transitions. Further, CMS states that while CoPs are a significant regulatory mechanism, noncompliance with one substandard within a CoP must be considered relative to the hospital's compliance with the other CoPs as well as the severity of the noncompliance and the risk it poses to patient health and safety. State surveyors are instructed that the determination of compliance depends upon the manner and degree to which the provider satisfies the standards within each condition.[10] CMS will issue interpretive guidelines and survey procedures for state surveyors prior to the effective date of this final rule, and the type of survey methods to be used is discussed. Finally, CMS notes that the patient event notification requirement requires only minimal information be provided.

As described earlier, the final rule provides that a reasonable effort must be made to provide the notification to specified recipients (primary care practitioner, group, entity, etc.) "which need to receive notification of the patient's status for treatment, care coordination, or quality improvement purposes." CMS states that this standard provides hospitals with the discretion to determine which recipients need to receive the notifications, taking individual provider preferences into account. For example, if a specific provider prefers to only receive notifications of patient discharge, nothing would preclude a hospital from limiting the notifications in that way. Or, if a provider has indicated that the notifications are not necessary or effective in supporting care coordination the hospital may decline to send them to that provider.

CMS believes that the patient event notification requirement being finalized complements and does not duplicate the discharge planning CoPs adopted in September 2019 because that rule does not require electronic transfer of patient medical information nor does it require the notification of appropriate providers regarding the patient's admission or discharge as this rule will do.

In responding to comments, CMS emphasizes that the rule does not require hospitals, psychiatric hospitals or CAHs to purchase or implement a new EHR system; it only requires that they demonstrate compliance with patient event notification if they use an electronic system that

[10] Readers are referred to the discussion of determining the severity of deficiencies found in Appendix A page 19 of the State Operations Manual available at https://www.cms.gov/media/423601

meets the HL7 2.5.1 content exchange standard. If they do not, the requirement does not apply. CMS believes that hospitals and surveyors will easily be able to determine whether this standard has been met and the requirement applies.

Further, while the requirement is that the HL7 2.5.1 standard ("ADT messaging standard") be met for purposes of determining whether the patient event notification rule applies to a hospital or CAH, CMS notes that it deliberately did not require hospitals use a specific standard to format or deliver patient event notifications; it does not require that hospitals use certified electronic health IT to send notifications. This flexibility is provided because CMS is aware of significant variation in how the ADT messages have been used for this purpose. It believes there are a variety of low-cost solutions that providers can use to meet the final rule requirements. CMS acknowledges that the use of different standards may impede the interoperability of this information exchange; that is, some providers may not be able to receive the patient event notifications hospitals are required to send under the final rule. CMS will consider how to encourage increased interoperability for the future.

With respect to comments discussing the challenges of patient matching, CMS recognizes this issue and the negative effects on patient event notification systems. It believes that the health IT industry should lead the way in developing innovating solutions to patient identity management, which will have many benefits beyond accurate patient event notification.

Some comments suggested that instead of requiring patient event notification, the Promoting Interoperability Program be used to advance these goals. CMS responds that the ONC certification program does not include a criterion for transmission of patient event notifications, and ONC does not believe there is a consensus standard for such transmission currently.

In the collection of information requirements section of the final rule, CMS estimates the costs to hospitals and CAHs of implementing the patient event notification requirement. Data collected in 2012 showed 59 percent of hospitals were routinely electronically transmitting patient event notifications. Projecting this forward, CMS assumes that between 29 and 71 percent of hospitals and CAHs will have to invest in updating their EHR systems under the final rule. Aggregate first year costs are estimated to range from $2.3 million to $5.7 million for hospitals and from $663,000 to $1.6 million for CAHs. These ranges for subsequent years are from $471,000 to $1.2 million for hospitals and $133,000 to $326,000 for CAHs.

XI.. Regulatory Impact Analysis

CMS estimates that the aggregate 10-year cost across payers of implementing and maintaining the API requirements in the final rule will total from $1.0 to $1.3 billion; the cost of implementing the increased federal-state data exchanges for dual-eligible care coordination is estimated to total $7 million over that period.

Table 8 reproduced from the final rule shows how the estimated costs of implementing and maintaining the API requirements would be distributed by year and program. For the mid-range (primary) estimate, 22% of the total cost is attributed to the QHPs; 33% to Medicaid and CHIP, and 45% to MA.

TABLE 8: API Costs (in millions) by Year and Program

Year	Full Implementation and Maintenance costs (millions) (From Table 5) For API provision	Individual Market Plans (22.19%)	Medicaid and CHIP (32.56%)	Medicare Advantage (45.24%)
2020 (Low estimate)	272.0	60.4	88.6	123.1
2020 (Primary estimate)	544.0	120.7	177.2	246.1
2020 (High Estimate)	816.0	181.1	265.7	369.2
2021	54.4	12.1	17.7	24.6
2022	54.4	12.1	17.7	24.6
2023	54.4	12.1	17.7	24.6
2024	54.4	12.1	17.7	24.6
2025	54.4	12.1	17.7	24.6
2026	54.4	12.1	17.7	24.6
2027	54.4	12.1	17.7	24.6
2028	54.4	12.1	17.7	24.6
2029	54.4	12.1	17.7	24.6
Total (Low Estimate)	761.5	169.0	248.0	344.6
Total (Primary Estimate)	1033.5	229.3	336.6	467.6
Total (High Estimate)	1305.5	289.7	425.1	590.7

The impact analysis discusses ways in which the different affected payers could transfer these new costs to enrollees, the states and the federal government. Additional tables in the final rule display these estimates; Table 15 shows the estimated annualized standards-based API implementation and maintenance costs that will be transferred to enrollee premiums, which range from $1.07 to $1.84 per enrollee.