Wynne Health Group

Memorandum

March 9, 2020

CMS, ONC Release Final Rules Addressing Interoperability, Information Blocking, EHR Certification Criteria

The Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator (ONC) released public inspection copies of much-anticipated parallel final rules (here and here, respectively) intended to advance interoperability and facilitate the exchange of electronic health information (EHI). In particular, the ONC rule also finalizes enhancements to its Health IT certification criteria, while setting forth definitions for activities that do not constitute "information blocking." The rules are being issued pursuant to the 21st Century Cures Act (Cures Act) and broader policies delineated in the President's 2017 Executive Order (EO).

- **What they are**. ONC's final rule outlines new standards for information blocking, adopts standards-based Application Programming Interfaces (API), and updates EHR certification criteria, and ongoing maintenance of EHR certification. The CMS final rule requires health plans in Medicare Advantage, Medicaid and the Children's Health Insurance Program (CHIP) fee for service (FFS) programs, Medicaid and CHIP managed care entities, and Qualified Health Plan (QHP) issuers in Federally-facilitated Exchanges (FFEs) to share claims data electronically with patients beginning January 1, 2021. Additionally, the rule addresses the secure exchange of electronic health record (EHR) data between health care providers to facilitate coordination of care.

- **Why they're important for you.** The ONC final rule codifies eight exceptions that would not constitute information blocking. ONC finalizes modifications to the 2015 Edition health IT certification criteria, including the addition of a standard for API-enabled services. ONC also finalizes voluntary certification criteria for pediatric health IT. Based on the standards outlined in the ONC rule, CMS finalizes requirements for payers and providers to share claims and health information with patients via a user-friendly electronic format through the Patient Access API; establishes a new Condition of Participation (CoP) for hospitals to provide notification to other providers and facilities regarding patient admissions, discharges, or transfers; and establishes new requirements for states to more frequently share data regarding dual eligible beneficiaries.

- **Potential next steps.** The ONC final rule will be implemented over the next 24 months. Compliance with the information blocking provision is required six months after publication of the final rule in the *Federal Register*, but penalties will not be imposed until pending civil monetary penalties (CMP) rules are final. Health IT developers have 24 months from publication to make technology certified to the updated criteria available to their customers. A detailed implementation timeline is available here. The CMS final rule will be effective 60 days after its formal publication;

however, the agency outlines a phased approach to implementation – please reference the CMS summary below for specific dates of applicability.

Highlights of the **ONC final rule** (fact sheets) include:

- **Information Blocking –** Driven by the Cures Act, ONC finalizes implementation of the law's information blocking provisions and finalizes eight exceptions to the definition of information blocking. Exceptions are reasonable and necessary activities that do not constitute information blocking by regulated actors, which as noted in the fact sheet, include health care providers, health IT developers of certified health IT, networks, and exchanges. Regulated actors are not required to comply with the information blocking provision until six months after publication of the final rule. Enforcement via civil monetary penalties will be determined through future notice and comment rulemaking by the Office of Inspector General. See finalized language beginning on p. 1225 of the public inspection copy and a fact sheet summary here. The exceptions are as follows:

  Exceptions that involve not fulfilling requests to access, exchange, or use EHI

  - **Preventing Harm Exception –** ONC finalizes an exception that allows a practice if the actor engaging in that practice holds a "reasonable belief" that it "will substantially reduce" a risk of harm to a patient or other persons. Regarding breadth, the practice must be "no broader than necessary" to substantially prevent harm. The practice must satisfy at least one condition from each of the following categories:

    - *Type of Risk* – The risk of harm must (1) "Be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination; or (2) arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason" (p. 1225-1226).
    - *Type of Harm* – The type of harm must satisfy one of the four conditions on p. 1226-1227. Of note, ONC cross-references these specific types of harm conditions to applicable harm standards in order to streamline compliance. See Table 3 on pp. 723-725 for more details.
    - *Implementation Basis* – The practice must be based on a determination consistent with a qualifying organizational policy or a determination specific to the facts and circumstances (p. 1227-1228).

    In addition, the practice must comply with the requirement that a patient has the right to request review of an individualized determination of risk of harm (p. 1227).

  - **Privacy Exception –** ONC finalizes an exception for practices reasonable and necessary to protect the privacy of an individual's EHI. See four "sub-exceptions" listed on p. 1228-12831. As highlighted in the fact sheet, these include (1) practices that satisfy

preconditions prescribed by privacy laws; (2) certain practices by a HEALTH IT developer of certified health IT not regulated by HIPAA but which implement documented and transparent privacy policies; (3) practices that are specifically permitted under HIPAA; (4) practices that respect an individual's privacy preferences. A regulated actor would need to qualify for at least one sub-exception to qualify for this exception.

- **Security Exception –** ONC finalizes an exception for security-related practices that meet the following conditions: (1) "must be directly related to safeguarding the confidentiality, integrity, and availability of EHI"; (2) "must be tailored to the specific security risk being addressed; (3) "must implement in a consistent and non-discriminatory manner" (p. 1231-1233). In addition, ONC requirements the practice to implement a qualifying organizational security policy or a qualifying security determination based on specific facts and circumstances.

- **Infeasibility Exception –** ONC finalizes an exception that allows a regulated actor to not comply with a request that is considered infeasible, due to one of the following: (1) an uncontrollable event (e.g., public health emergency, natural or human-made disaster); (2) "the actor cannot unambiguously segment the requested EHI" from EHI that is prohibited from being shared or allowed to be withheld; or (3) "through a contemporaneous written record or other documentation," the actor demonstrates its process for considering certain factors (e.g., type of EHI requested, cost and available financial resources) in determining the request would not be feasible. The actor must respond in writing to the requestor within 10 business days of receipt of the request the reason(s) why the request is infeasible (p. 1233-1234).

- **Health IT Performance Exception –** ONC finalizes an exception that allows a practice implemented to maintain or improve health IT performance, provided it meets the following requirements: (1) it is implemented for a period no longer than necessary to perform the required maintenance or improvements; (2) implemented in a consistent and non-discriminatory manner; and (3) complies with certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN (p. 1235-1236).

  In addition, ONC finalizes a policy allowing an actor to take action against a third-party application that negatively impacts the health IT's performance. If the unavailability is in response to a risk of harm or security risk, the actor does not need to meet these requirements and must only comply with the requirements of the Preventing Harm and Security Exception.

Exceptions that involve fulfilling requests to access, exchange, or use EHI

- **Content and Manner Exception** – ONC finalized a new exception (not included in the proposed rule) that allows the practice of limiting content of its response to or the manner in which it is fulfills a request (p. 1236-1238). For up to 24 months after the publication

date of the final rule, the actor must respond with, at a minimum, the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard. On or after the 24-month period, the actor must respond to request as required. The actor must fulfill a request in the manner requested, unless the actor lacks the technical capacity to do so or cannot reach agreeable terms with the requestor. The actor must then fulfill the request through an alternative manner without unnecessary delay using certified technology, content and transport standards, and a machine-readable format. Additionally, the actor must also satisfy the Fees Exception and Licensing Exception.

- **Fees Exception –** ONC finalized an exception that allows an actor to charge fees, in order to recover costs that were reasonably incurred to develop technologies and provide services aimed at improving interoperability (p. 1238-1240). The fees must be (1) "based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests"; (2) "reasonably related to the actor's costs of providing the type of access, exchange, or use of electronic health information to, or at the request of, the person or entity to whom the fee is charged; (3) "reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported; and (4) "based on costs not otherwise recovered for the same instance of service to a provider and third party." Of note, the exception does not apply to (1) a fee prohibited by the HIPAA Privacy Rule; (2) a fee based on the electronic access by an individual to his or her EHI; (3) a fee for exporting EHI via the capability of certified health IT for the purposes of switching health IT or to provide patients their EHI; and (4) a fee for exporting or converting data from an EHR technology that was not agreed to in writing at the time technology was acquired.

- **Licensing Exception –** ONC finalizes an exception that allows a regulated actor to license interoperability elements and earn return if the actor begins license negotiation with the request within 10 business days from receipt of the request and negotiates a license within 30 business days from receipt of the request. The license must satisfy conditions relating to scope of rights, reasonable royalty, non-discriminatory terms, collateral terms, and non-disclosure agreements. In addition, the actor is prohibited from engaging in a practice that (1) impedes the efficient use of interoperability elements; (2) impedes the efficient development, distribution, deployment, or use of an interoperable productor service; or (3) degrades the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after providing the licensee with a reasonable opportunity to updates its technology in order to maintain interoperability (p. 1240-1243).

- **Electronic Health Information:** To avoid confusion among providers between the ONC definition and what is already defined in the HIPAA law, ONC is finalizing its definition of electronic health information (EHI) to equate to electronic protected health information (ePHI) as defined in HIPAA and codified at 45 CFR 160.103. See p. 629 for more. The newly defined and finalized "Content and Manner" exception, will allow actors time to adjust to providing the full

scope of EHI for access, exchange, and use based on the HIPAA-compliant definition of ePHI. See p. 588 for more.

- **Illustrative Practices that May Implicate Information Blocking:** Beginning on p. 659, ONC notes that the illustrative examples it provided in its proposed rule of what could constitute information blocking were non-exhaustive and meant to provide greater clarity on the array of practices that could implicate information blocking. While it received requests to revise or clarify these examples, ONC elected not to update a "majority" of these examples, as it believes most are "still applicable."

  However, the subsequent discussion in the final rule includes "necessary clarifications" regarding certain concepts included in the original set of proposed examples. These clarifications pertain to scenarios involving restrictions on access, exchange, or use (p. 659); limiting or restricting the interoperability of Health IT (p. 664); impeding innovations and advancements in access, exchange, or use or Health IT-enabled care delivery (p. 669); rent-seeking and other opportunistic pricing practices (p. 684); and, non-standard implementation practices (p. 686).

- **Conditions and Maintenance of Certification:** ONC is finalizing seven Conditions of Certification for health IT developers, pursuant to those outlined in section 4002 of the Cures Act. Noncompliance with these requirements will be subject to ONC direct review, corrective action, and enforcement procedures under the ONC Health IT Certification Program (the Program). ONC states that in the most extreme cases it may ban a health IT developer from the Program and/or terminate the certification of one or more of its Health IT modules.

  Details on the seven conditions follow.

  - **Information Blocking –** A health IT developer may not take any action that constitutes information blocking as defined in section 3022(a) of the Public Health Service Act.

  - **Assurances –** A health IT developer must provide assurances to the Secretary, through the several Conditions of Certification for the Program, that it will not take any action that constitutes information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI.

  - **Communications –** A health IT developer may not restrict communications about certain aspects of the performance of health IT and any related business practices. ONC is finalizing this condition with narrow exceptions allowing for restricted communications when such communications would infringe on the health IT developer's intellectual property rights. Health IT developers may not, therefore, impose any contractual requirements contravening these requirements. They must also notify all affected customers or other affected entities that they will not be enforcing any such contractual provisions if the developer already has a contract in effect with stipulations that contravene these requirements.

- **Application Programming Interfaces (APIs) –** A health IT developer must publish APIs that allow "health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards."

- **Real World Testing of Certified Health IT –** A health IT developer must test the real-world use of its health IT for interoperability in the types of settings in which the technology would be marketed.

- **Attestations –** A health IT developer must provide an attestation of compliance with the Conditions and Maintenance of Certification, except for the "EHR reporting criteria submission" Condition of Certification. Developers will attest twice a year and submit them to ONC-ACBs.

- **EHR Reporting Criteria Submission** – ONC states that the Cures Act requires health IT developers to submit reporting criteria on certified health IT. However, ONC has not yet established such a program. Once ONC develops an EHR reporting program, the agency states, it will engage in rulemaking to implement an associated Condition and Maintenance of Certification requirements for health IT developers.

The full discussion begins on p. 292. A separate fact sheet with additional detail on the APIs Conditions and Maintenance of Certification is available here.

- **Updates to the 2015 Edition Certification Criteria** – As summarized beginning on p. 10 of the final rule, and discussed in greater detail beginning on p. 87, ONC is finalizing the following revisions and updates to the 2015 Edition:

  - **Adoption of the USCDI as a Standard** – ONC is finalizing removal of the "Common Clinical Data Set" (CCDS) definition and its references from the 2015 Edition and replacing it with the "United States Core Data for Interoperability" (USCDI) as a standard, naming it USCDI Version 1 (or USCDI v1).

  - **Electronic Prescribing** – ONC is finalizing an update to the electronic prescribing (e-Rx) SCRIPT standard to NCPDP SCRIPT 2017071. They are also adopting a new certification criterion for e-Rx, in alignment with the CMS Part D standards to NCPDP SCRIPT 2017071 for e-RX and medical history (MH).

  - **Clinical Quality Measures** – ONC is finalizing removal of the HL7 Quality Reporting Document Architecture (QRDA) standard requirements from the 2015 Edition "CQMs – report" criterion and, in their place, requiring Health IT Modules to support the CMS QRDA Implementation Guide (IGs).

  - **Electronic Health Information Export** – ONC is finalizing, with modifications, a new 2015 Edition certification criterion for "EHI export," which would replace the 2015 Edition

"data export" certification criterion and become part of the 2015 Edition Base EHR definition. The modifications refine the scope of the data which must be exported and aligns the criterion to the finalized definition of EHI. ONC did not finalize inclusion of EHI Export in the 2015 Edition Base EHR definition as proposed.

- **Application Programming Interfaces (APIs)** – ONC is finalizing the adoption of a new API criterion that will replace the "application access – data category request" certification criterion and become part of the 2015 Edition Base EHR definition, and requires the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications.

- **Privacy and Security Transparency Attestations** – ONC is adopting two new privacy and security transparency attestation certification criteria, which would identify whether certified health IT supports encrypting authentication credentials and/or multifactor authentication. In order to be issued a certification, ONC is finalizing a requirement that a Health IT Module developer attest to whether the Health IT Module encrypts authentication credentials and whether the Health IT Module supports multi-factor authentication.

- **Data Segmentation for Privacy and Consent Management** – ONC is finalizing the removal of two existing 2015 Edition "data segmentation for privacy" (DS4P) certification criteria, and is replacing them with two new criteria for C-CDA that would support a more granular approach to privacy tagging data consent management for health information exchange supported by either the C-CDA-based exchange standards. ONC is not finalizing its proposal to add a new 2015 Edition certification criterion, "consent management for APIs," in response to stakeholder comments.

- **Deregulation** – ONC reviewed and evaluated existing regulations to identify opportunities for deregulation that would reduce provider burden. As a result, ONC is finalizing five deregulatory actions:

  - **Removal of Randomized Surveillance Requirements** – ONC finalizes eliminating certain surveillance requirements that ONC-Authorized Certification Bodies (ONC-ACBs) must perform. Eliminating such requirements, ONC says, will allow ONC-ACBs more flexibility to identify the right approach for surveillance actions. Details on the finalized provisions for elimination are on p. 48.

  - **Removal of the 2014 Edition from the Code of Federal Regulations (CFR)** – Noting the 2014 Edition is now outdated, ONC finalizes its elimination, which would render the 2015 Edition the baseline for health IT certification. A further discussion of the benefits associated with eliminating the 2014 Edition begins on p. 53.

  - **Removal of the ONC-Approved Accreditor (ONC-AA) from Program** – ONC notes they have found the ONC-AA's role no longer necessary, and therefore finalize its

elimination. Though initially created to oversee the activities of ONC-ACBs, ONC finds its role to be duplicative of ONC's own oversight responsibilities. Details of the ONC-AA's finalized elimination begins on p. 56.

- **Removal of Certain 2015 Edition Certification Criteria and Standards** – ONC also finalizes the removal of a series of criteria and standards in the 2015 Edition. This, ONC states, will eliminate the need for providers to "design and meet specific certification functionalities; prepare, test, and certify health IT in certain instances; adhere to associated reporting and disclosure requirements; maintain and update certifications for certified functionalities; and participate in surveillance of certified health IT." ONC finalized making changes to the following certification criteria: base EHR definition, drug formulary and preferred drug lists, patient-specific education resources, CCDS summary record – create and receive, and secure messaging. Details on the specific changes begin on p. 58.

- **Removal of Certain Certification Program Requirements** – ONC finalizes the removal of "certain mandatory disclosure requirements and a related attestation requirement under the Program." ONC expects this will lead to reduced costs and burden for stakeholders particularly developers and ONC-ACBs. The finalized items for removal are limitation disclosures and transparency and mandatory disclosures requirements. The agency details that the removal of these disclosures is no longer necessary and removal is appropriate to reduce administrative burden for health IT developers. The ONC further notes that they did not propose and did not finalize a complete removal of transparency requirements. Additional details are on p. 80.

The ONC did not finalize a sixth deregulatory action related to the recognition of the Food and Drug Administration (FDA) Software Precertification Program due to comments that indicated that finalization would be premature.

- **Health IT for Pediatrics** – To implement Section 4001(b) of the Cures Act, ONC is finalizing 10 recommended requirements for voluntary certification of health IT in the pediatric setting (see pp. 281-282). The first eight recommendations reflect a synthesis of critical data elements identified by the Children's Model EHR Format – a collaborative tool developed by several agencies within the Department of Health and Human Services and external organizations – as well as by the American Academy of Pediatrics. ONC added the latter two recommendations: "track incomplete preventive care opportunities" and "flag special health care needs" to address items that were important to pediatric stakeholders and are related to other items within the Children's Format.

  To facilitate the adoption of the 10 recommendations, ONC is developing a Pediatric Health IT Developer Informational Resource and a Pediatric Health IT Provider Information Resource to be available for use in 2020 (p. 284). The agency notes that they will continue to work with stakeholders when considering technical and implementation recommendations.

Additionally, ONC is finalizing the adoption of the 2015 Edition Certification Criteria to facilitate implementation of the aforementioned recommendations. ONC also finalized four new 2015 Edition criteria to further support pediatric health care providers: Application Programming Interface (API) based on Fast Healthcare Interoperability Resources (FHIR), data segmentation for privacy, electronic prescribing certification, and United States Core Data Set for Interoperability (USCDI). See further discussion beginning on p. 285.

- **Data Exchange Between EHRs and Registries** – In the proposed rule, ONC issued a Request for Information (RFI) on how an FHIR standard-based API may better facilitate data exchange between EHRs and registries. In the final rule, the ONC notes they received 75 comments in response to the RFI, and the agency is considering including this information in future rule making (p. 1016).

Highlights of the **CMS** final rule (fact sheet) include:

- **Patient Access API** – CMS finalizes the requirement for certain payers – (MA organizations, Medicaid FFS programs, Medicaid managed care plans, CHIP FFS programs, CHIP managed care entities, and QHP issuers on the FFEs) – to implement and maintain a secure, standards-based API (HL7 FHIR Release 4.0.1, in accordance with the ONC rule), that allows patients to easily access their claims and encounter information, including cost, as well as a defined sub-set of their clinical information through third-party applications of their choice. Specifically, the Patient Access API must, at a minimum, make available adjudicated claims (including provider remittances and enrollee cost-sharing); encounters with capitated providers; and clinical data, including laboratory results (when maintained by the impacted payer). Data must be made available no later than one business day after a claim is adjudicated or encounter data are received. Impacted payers must implement the Patient Access API beginning January 1, 2021 (or for QHP issuers on the FFEs, for plan years beginning on or after January 1, 2021), at which time they should make available the specified data they maintain with a date of service back to January 1, 2016 and forward. Note that these requirements exclude issuers offering only Stand-alone dental plans (SADPs) and QHP issuers offering coverage in the Federally-facilitated Small Business Health Options Program (FF-SHOP). See p. 54.

- **Provider Directory API** – Beginning on p. 186, CMS finalizes the requirement that impacted providers make standardized information about their provider networks available through a Provider Directory API that is compliant with the technical standards finalized in the ONC rule (again (FHIR)-based), and is accessible via a public-facing digital endpoint on the payer's website to ensure public discovery and access. At a minimum, this data must include provider names, addresses, phone numbers, and specialties. For MA organizations that offer MA-PD plans, they must also make available, at a minimum, pharmacy directory data, including the pharmacy name, address, phone number, number of pharmacies in the network, and mix (specifically the type of pharmacy, such as "retail pharmacy"). Access to the published Provider Directory API must be fully implemented by January 1, 2021, and payers will have 30 calendar days to add or update directory information when they receive new data. CMS notes that QHP issuers on the FFEs are already required to make provider directory information available in a specified, machine-readable format, and therefore they are excused from this requirement.

- **Provider Failure to Report Digital Contact Information** – CMS also finalized its proposal to publicly identify the names and NPIs of clinicians who have not submitted digital contact information via the National Plan and Provider Enumeration System (NPPES), beginning in the second half of 2020 (see p. 280).

- **Payer-to-Payer Data Exchange** – On p. CMS finalizes, with modifications, its proposal to require impacted payers to exchange certain patient clinical data (specifically the U.S. Core Data for Interoperability (USCDI) version 1 data set) at the patient's request, allowing the patient to take their information with them as they move from payer to payer and provider to provider over time, to create a cumulative health record with their current payer. Consistent with the Patient Access API, issuers will be required (at the consumer's request) to furnish any information they have maintained for such current or former enrollee with a date of service dating back to January 1, 2016. This information must be furnish to any other payer identified by the current or former enrollee; however, CMS finalizes a provision intended to reduce burden which states that a payer is only obligated to share data received from another payer under this regulation in the electronic form and format it was received. This process for data exchange must be implemented beginning January 1, 2022 (or for QHP issuers on the FFEs, plan years beginning on or after January 1, 2022). See. p. 204.

- **Payer Participation in Trusted Exchange Networks** – Beginning on p. 222, CMS discusses its decision not to finalize its proposal to require impacted payers to participate in a trusted exchange network given concerns that commenters raised regarding the need for a mature Trusted Exchange Framework and Common Agreement (TEFCA) to be in place first.

- **Dual-eligibles and Information Exchange –** CMS finalizes, as proposed, a requirement that states exchange certain Medicare/Medicaid information on dual-eligible beneficiaries on a daily basis, rather than on a monthly basis. This includes data related to Medicare "buy-in" (or, Medicare Savings Programs) program beneficiaries (details) and other stipulated data (MMA file data for duals). CMS maintains that the more frequent exchange of information will improve the accuracy of the data, and therefore, improve how the state and CMS eligibility and Medicaid Management Information System (MMIS) systems work together. See the discussion beginning on p. 226 of the public inspection copy.

- **Information Blocking and Public Reporting –** On p. 255, CMS finalizes, as proposed, a policy to include an indicator on Physician Compare for the eligible clinicians and groups that submit a "no" response to any of the three prevention of information blocking attestation statements for MIPS. On p. 264, the agency also finalizes, as a proposed, a policy to include information on a CMS website than an eligible hospital or critical access hospital (CAH) submitted a "no" response to any of the three prevention of information blocking attestation statements. An eligible hospital or CAH will have a 30-day period to review the information before it is publicly posted. CMS notes that it may consider revising the information on a case-by-case basis. See fact sheet on the CY 2017 Quality Payment Program final rule for more details on the information blocking attestation statements.

- **Care Coordination: Admission, Discharge, and Transfer Event Notifications** – On p. 280, CMS finalizes its proposal to require, as part of hospitals' (including psychiatric hospitals and critical access hospitals (CAHs)) Conditions of Participation (CoP), electronic patient event notifications of a patient's admission, discharge, and/or transfer to another health care facility or provider. The agency notes that a hospital will be subject to these requirements if it uses a system that conforms with the HL7 2.5.1 content exchange standard, which indicates a system has the basic capacity to generate information for patient event notifications. Further, CMS states that a hospital system's ability to meet the ADT standard will be used only to determine whether a hospital is subject to the CoP.

  Requirements for the content and format of the patient event notifications are limited to minimal information elements and CMS did not propose a specific format or standard. However, the agency does specify that a hospital must demonstrate that its system sends notifications at the time of a patient's registration in the emergency department or admission to inpatient services, and also prior to, or at the time of, a patient's discharge and/or transfer from the emergency department or inpatient services, to all applicable post-acute care services providers and suppliers, primary care practitioners and groups, and other practitioners and groups identified by the patient as primarily responsible for his or her care, and who or which need to receive notification of the patient's status for treatment, care coordination, or quality improvement purposes. This policy will take effect six months after publication of the rule.

- **Effective Dates** – CMS outlines the following applicability dates by provision of the final rule:

  - Admission, Discharge, and Transfer Event Notifications (applicable fall 2020)
  - Public Reporting and Information Blocking (applicable late 2020)
  - Digital Contact Information (applicable late 2020)
  - Patient Access API (applicable January 1, 2021)
  - Provider Directory API (applicable January 1, 2021)
  - Payer-to-Payer Data Exchange (applicable January 1, 2022)
  - Improving the Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges (applicable April 1, 2022)