spg SACHS POLICY GROUP
60 East 42nd Street, Suite 1762
New York, NY 10165
Phone: 212 827 0660
Fax: 212 827 0667

Interoperability and Patient Access Final Rule

OVERVIEW

On March 9th, the Centers for Medicare and Medicaid Services (CMS) finalized a rule that requires health plans participating in Medicare Advantage (MA), Medicaid, the Children's Health Insurance Program (CHIP), and the federally facilitated exchanges (FFEs) to share claims data electronically with patients and other health plans at a patient's request. The rule also finalizes certain provider requirements for electronic information sharing, including requirements related to notification for patient admission, discharge and transfer.

The final rule is available here.

APPLICATION PROGRAMMING INTERFACES (API)

Patient Access API

The rule requires MA organizations, Medicaid and CHIP fee for service programs, Medicaid and CHIP managed care plans, and qualified health plan (QHP) issuers on the FFEs to implement and maintain a standards-based Patient Access API that meets the technical standards finalized by HHS in the ONC 21st Century Cures Act final rule. Through the API, payers must allow third-party applications to retrieve data at the request of enrollees.

At a minimum, the Patient Access API must allow third-party applications to retrieve:

- Adjudicated claims, including remittances and enrollee cost-sharing;
- Capitated provider encounters; and
- Clinical data and laboratory results.

The rule is requiring that the above data be made available within one business day after a claim is adjudicated or encounter data is received. Additionally, starting January 1st, 2021, all data with a date of service on or after January 1st, 2016, must be made available through the Patient Access API.

Provider Directory API

The rule also requires that MA organizations, Medicaid and CHIP FFS programs, Medicaid managed care plans, and CHIP managed care entities make standardized information about their provider networks available through a Provider Directory API. QHPs are excluded due to existing requirements to supply provider directory information to the FFEs. The Provider Directory API must conform with the same technical standards as the Patient Access API, excluding the security protocols that restrict information to particular individuals or organizations. The Provider Directory API must be accessible via a public-facing digital endpoint on the payer's website.

At a minimum, the Provider Directory API must display:

- Provider names;
- Provider addresses;
- Provider phone numbers;

60 East 42nd Street, Suite 1762
New York, NY 10165
Phone: 212 827 0660
Fax: 212 827 0667

- Provider specialties; and
- Pharmacy directory data, if an MA organization offers a prescription drug plan.

The rule requires that all directory information must be made available to current and prospective enrollees and the public through the Provider Directory API within 30 calendar days of a payer receiving provider directory information or an update to the provider directory information. Like the Patient Access API, the Provider Directory API must be fully implemented by January 1st, 2021.

API Access Exceptions

Similar to the ONC's Interoperability and Data Blocking rule, this final rule permits certain exceptions to the requirement to provide requested patient information. A payer could deny access to the API if it reasonably determined that allowing the app to connect or remain connected to the API would present an unacceptable level of risk to the security of PHI on the payer's systems, consistent with the payer's HIPAA Security Rule obligations and based on objective, verifiable criteria that would be applied fairly and consistently across all applications through which enrollees seek to access their electronic health information, including but not limited to criteria that may rely on automated monitoring and risk mitigation tools.

Payers should take reasonable measures to protect data in transit, unless an individual expressly asks that the information be conveyed in an unsecure form, and after the individual has been warned of and accepted the risks associated with the unsecure transmission. More generally, payers will be required to inform patients of the possible risk of sharing their data with third-party apps.

Payers may not restrict third party access to the API on other bases, such as the lack of a Business Associate Agreement if the third party is not a covered entity under HIPAA, so long as the third party is acting on behalf of a patient-initiated request for that patient's own personal health data. Regulation of the how the data is used by the third party once received, if it is not a HIPAA covered entity, was deemed beyond the scope of CMS regulation, though CMS referred to Federal Trade Commission (FTC) regulations that regulate deceptive business practices (the FTC has oversight over such apps).

CMS declined requests to develop a national app certification program to establish a safe list of third parties, and encouraged the payer and tech industries to collaborate to reduce administrative burden in the security risk vetting process.

PAYER-TO-PAYER DATA EXCHANGE

The rule requires that all states participate in a daily exchange of buy-in data, in which they send data in the form of a Medicare Modernization Act (MMA) file, and receive responses from CMS on a daily basis. This provision aims to improve the ability of providers and payers to coordinate eligibility, enrollment, benefits, and care for dually eligible individuals.

PROVIDER INFORMATION BLOCKING INDICATORS

The rule updates Physician Compare by including an indicator for the eligible clinicians and groups that submit a "no" response to any of the three prevention of information blocking statements for MIPS. The indicator will be posted starting with the 2019 performance period data available for reporting later this year. Additionally, CMS will include information on a publicly available website that indicates that an eligible hospital or critical access hospital (CAH) attesting under the Medicare FFS Promoting

60 East 42nd Street, Suite 1762
New York, NY 10165
Phone: 212 827 0660
Fax: 212 827 0667

Interoperability Program had submitted a "no" response to any of the three attestation statements related to the prevention of information blocking.

If eligible clinicians and groups, or eligible hospitals and CAHs leave a "blank" response to the attestation statements related to the prevention of information blocking, the attestations will be considered incomplete, and no information will be posted.

ELECTRONIC MEDICAL RECORDS SYSTEM NOTIFICATION REQUIREMENTS

The rule requires that, within six month of publication, hospitals, psychiatric hospitals, and CAHs that utilize an electronic medical records system or electronic administrative system demonstrate that:

- Its system sends admission, discharge, and/or transfer notifications directly to all applicable post-acute care services providers and suppliers, primary and other care practitioners and groups identified by the patient as responsible for his or her care, and who need to receive notification of the patient's status for treatment, care coordination, or quality improvement purposes;
- Its system sends notifications that must include a minimum set of patient health information; and
- Its system's notification capacity is fully operational and that it operates in accordance with all state and federal statutes and regulations regarding the exchange of patient health information.

NPPES SYTEM UPDATES

The rule finalizes the proposal to publicly report the names and National Provider Identifier (NPI) numbers of providers who do not have digital contact information included in the National Plan and Provider Enumeration System (NPPES) beginning in the second half of 2020.