healthcare prepayment plans under section 1833 of the Act, and network PFFS plan types.

(*iv*) Calculates penetration at the contract ID and county level by dividing the number of enrollees for a given contract ID and county by the number of eligible beneficiaries in that county.

(*v*) Groups counties by county designation to determine the 95th percentile of penetration among MA plans for each county type.

(f) *Exception requests.* (1) An MA plan may request an exception to network adequacy criteria in paragraphs (b) through (e) of this section when both of the following occur:

(i) Certain providers or facilities are not available for the MA plan to meet the network adequacy criteria as shown in the Provider Supply file for the year for a given county and specialty type.

(ii) The MA plan has contracted with other providers and facilities that may be located beyond the limits in the time and distance criteria, but are currently available and accessible to most enrollees, consistent with the local pattern of care.

(2) In evaluating exception requests, CMS considers whether—

(i) The current access to providers and facilities is different from the HSD reference and Provider Supply files for the year;

(ii) There are other factors present, in accordance with §422.112(a)(10)(v), that demonstrate that network access is consistent with or better than the original Medicare pattern of care; and

(iii) Approval of the exception is in the best interests of beneficiaries.

[85 FR 33904, June 2, 2020]

### § 422.118 Confidentiality and accuracy of enrollee records.

For any medical records or other health and enrollment information it maintains with respect to enrollees, an MA organization must establish procedures to do the following:

(a) Abide by all Federal and State laws regarding confidentiality and disclosure of medical records, or other health and enrollment information. The MA organization must safeguard the privacy of any information that identifies a particular enrollee and have procedures that specify—

(1) For what purposes the information will be used within the organization; and

(2) To whom and for what purposes it will disclose the information outside the organization.

(b) Ensure that medical information is released only in accordance with applicable Federal or State law, or pursuant to court orders or subpoenas.

(c) Maintain the records and information in an accurate and timely manner.

(d) Ensure timely access by enrollees to the records and information that pertain to them.

[65 FR 40323, June 29, 2000]

### § 422.119 Access to and exchange of health data and plan information.

(a) *Application Programming Interface to support MA enrollees.* A Medicare Advantage (MA) organization must implement and maintain a standards-based Application Programming Interface (API) that permits third-party applications to retrieve, with the approval and at the direction of a current individual MA enrollee or the enrollee's personal representative, data specified in paragraph (b) of this section through the use of common technologies and without special effort from the enrollee.

(b) *Accessible content.* (1) An MA organization must make the following information accessible to its current enrollees or the enrollee's personal representative through the API described in paragraph (a) of this section:

(i) Data concerning adjudicated claims, including claims data for payment decisions that may be appealed, were appealed, or are in the process of appeal, and provider remittances and enrollee cost-sharing pertaining to such claims, no later than one (1) business day after a claim is processed;

(ii) Encounter data from capitated providers, no later than one (1) business day after data concerning the encounter is received by the MA organization; and

(iii) Clinical data, including laboratory results, if the MA organization maintains any such data, no later than one (1) business day after the data is received by the MA organization.

(2) In addition to the information specified in paragraph (b)(1) of this section, an MA organization that offers an MA–PD plan must make the following information accessible to its enrollees through the API described in paragraph (a) of this section:

(i) Data concerning adjudicated claims for covered Part D drugs, including remittances and enrollee cost-sharing, no later than one (1) business day after a claim is adjudicated; and,

(ii) Formulary data that includes covered Part D drugs, and any tiered formulary structure or utilization management procedure which pertains to those drugs.

(c) *Technical requirements.* An MA organization implementing an API under paragraph (a) of this section:

(1) Must implement, maintain, and use API technology conformant with 45 CFR 170.215;

(2) Must conduct routine testing and monitoring, and update as appropriate, to ensure the API functions properly, including assessments to verify that the API is fully and successfully implementing privacy and security features such as, but not limited to, those required to comply with HIPAA privacy and security requirements in 45 CFR parts 160 and 164, 42 CFR parts 2 and 3, and other applicable law protecting the privacy and security of individually identifiable data;

(3) Must comply with the content and vocabulary standard requirements in paragraphs (c)(3)(i) and (ii) of this section, as applicable to the data type or data element, unless alternate standards are required by other applicable law:

(i) Content and vocabulary standards at 45 CFR 170.213 where such standards are applicable to the data type or element, as appropriate; and

(ii) Content and vocabulary standards at 45 CFR part 162 and §423.160 of this chapter where required by law or where such standards are applicable to the data type or element, as appropriate.

(4) May use an updated version of any standard or all standards required under paragraph (c)(1) or (3) of this section, where:

(i) Use of the updated version of the standard is required by other applicable law; or

(ii) Use of the updated version of the standard is not prohibited under other applicable law, provided that:

(A) For content and vocabulary standards other than those at 45 CFR 170.213, the Secretary has not prohibited use of the updated version of a standard for purposes of this section or 45 CFR part 170;

(B) For standards at 45 CFR 170.213 and 45 CFR 170.215, the National Coordinator has approved the updated version for use in the ONC Health IT Certification Program; and

(C) Use of the updated version of a standard does not disrupt an end user's ability to access the data described in paragraph (b) of this section through the API described in paragraph (a) of this section.

(d) *Documentation requirements for APIs.* For each API implemented in accordance with paragraph (a) of this section, an MA organization must make publicly accessible, by posting directly on its website or via publicly accessible hyperlink(s), complete accompanying documentation that contains, at a minimum the information listed in this paragraph. For the purposes of this section, ''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 a fee for access to the documentation; a requirement to receive a copy of the material via email; a requirement to register or create an account to receive the documentation; or a requirement to read promotional material or agree to receive future communications from the organization making the documentation available;

(1) 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;

(2) The software components and configurations an application must use in order to successfully interact with the API and process its response(s); and

(3) All applicable technical requirements and attributes necessary for an

application to be registered with any authorization server(s) deployed in conjunction with the API.

(e) *Denial or discontinuation of access to the API.* An MA organization may deny or discontinue any third party application's connection to the API required under paragraph (a) of this section if the MA organization:

(1) 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 MA organization's systems; and

(2) 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, as defined at 45 CFR 171.102, including but not limited to criteria that may rely on automated monitoring and risk mitigation tools.

(f) *Coordination among payers.* (1) An MA organization must maintain a process for the electronic exchange of, at a minimum, the data classes and elements included in the content standard adopted at 45 CFR 170.213. Such information received by an MA organization must be incorporated into the MA organization's records about the current enrollee. With the approval and at the direction of a current or former enrollee or the enrollee's personal representative, the MA organization must:

(i) Receive all such data for a current enrollee from any other payer that has provided coverage to the enrollee within the preceding 5 years;

(ii) At any time an enrollee is currently enrolled in the MA plan and up to 5 years after disenrollment, send all such data to any other payer that currently covers the enrollee or a payer the enrollee or the enrollee's personal representative specifically requests receive the data; and

(iii) Send data received from another payer under this paragraph (f) in the electronic form and format it was received.

(2) [Reserved]

(g) *Enrollee resources regarding privacy and security.* An MA organization must provide in an easily accessible location on its public website and through other appropriate mechanisms through which it ordinarily communicates with current and former enrollees seeking to access their health information held by the MA organization, educational resources in non-technical, simple and easy-to-understand language explaining at a minimum:

(1) 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

(2) An overview of which types of organizations or individuals are and are not likely to be HIPAA covered entities, the oversight responsibilities of the Office for Civil Rights (OCR) and the Federal Trade Commission (FTC), and how to submit a complaint to:

(i) The HHS Office for Civil Rights (OCR); and

(ii) The Federal Trade Commission (FTC).

(h) *Applicability.* (1) An MA organization must comply with the requirements in paragraphs (a) through (e) and (g) of this section beginning January 1, 2021, and with the requirements in paragraph (f) beginning January 1, 2022 with regard to data:

(i) With a date of service on or after January 1, 2016; and

(ii) That are maintained by the MA organization.

(2) [Reserved]

[85 FR 25632, May 1, 2020]

### § 422.120 Access to published provider directory information.

(a) An MA organization must implement and maintain a publicly accessible, standards-based Application Programming Interface (API) that is conformant with the technical requirements at § 422.119(c), excluding the security protocols related to user authentication and authorization and any