

(3) Continue to be accessible for the duration that the authorization is active and at least 1 year after the prior authorization's last status change.

(v) Drugs are defined for the purposes of paragraph (b)(1)(iv) of this section as any and all drugs covered by the MA organization, including any products that constitute a Part D drug, as defined by §423.100 of this chapter, and are covered under the Medicare Part D benefit.

(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 and maintain API technology conformant with 45 CFR 170.215(a)(1), (b)(1)(i), (c)(1), and (e)(1);

(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) Using the updated version of the standard, implementation guide, or specification does not disrupt an end user's ability to access the data specified in paragraph (b) of this section or §§422.120, 422.121, and 422.122 through the required APIs.

(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 apps and developers through which parties seek to access electronic health information, as defined in 45 CFR 171.102, including but not limited to, criteria that rely on automated monitoring and risk mitigation tools.

(f) *Reporting on Patient Access API usage.* Beginning in 2026, by March 31 following any calendar year that it offers an MA plan, an MA organization must report to CMS the following metrics, in the form of aggregated, de-identified data, for the previous calendar year at the contract level in the form and manner specified by the Secretary:

(1) The total number of unique enrollees whose data are transferred via the Patient Access API to a health app designated by the enrollee.

(2) The total number of unique enrollees whose data are transferred more

than once via the Patient Access API to a health app designated by the enrollee.

(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.* An MA organization must comply with the requirements of this section beginning in paragraphs (a) through (e) and (g) of this section beginning January 1, 2021, unless otherwise specified, and with the requirements in paragraph (f) of this section beginning in 2026, with regard to data:

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

(2) That are maintained by the MA organization.

[85 FR 25632, May 1, 2020, as amended at 89 FR 8974, Feb. 8, 2024]

§ 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