

(b) CMS will notify the qualified entity when the entity's proposed changes are approved or denied for use, generally within 30 days of the qualified entity submitting the changes to CMS. If a CMS decision on approval or disapproval for a change is not forthcoming within 30 days and CMS does not request an additional 30 days for review, the change or modification shall be deemed to be approved.

(c) If the amount of claims data from other sources available to a qualified entity decreases, the qualified entity must immediately inform CMS and submit documentation that the remaining claims data from other sources is sufficient to address the methodological concerns regarding sample size and reliability. Under no circumstances may a qualified entity use Medicare data to create a report, use a measure, or share a report after the amount of claims data from other sources available to a qualified entity decreases until CMS determines either that the remaining claims data is sufficient or that the qualified entity has collected adequate additional data to address any deficiencies.

(1) If the qualified entity cannot submit the documentation required in paragraph (c) of this section, or if CMS determines that the remaining claims data is not sufficient, CMS will afford the qualified entity up to 120 days to obtain additional claims to address any deficiencies. If the qualified entity does not have access to sufficient new data after that time, CMS will terminate its relationship with the qualified entity.

(2) If CMS determines that the remaining claims data is sufficient, the qualified entity may continue issuing reports, using measures, and sharing reports.

**§401.713 Ensuring the privacy and security of data.**

(a) *Data use agreement between CMS and a qualified entity.* A qualified entity must comply with the data requirements in its data use agreement with CMS (hereinafter the CMS DUA). Contractors (including, where applicable, business associates) of qualified entities that are anticipated to have access to the Medicare claims data or beneficiary identifiable data in the context

of this program are also required to execute and comply with the CMS DUA. The CMS DUA will require the qualified entity to maintain privacy and security protocols throughout the duration of the agreement with CMS, and will ban the use or disclosure of Medicare data or any derivative data for purposes other than those set out in this subpart. The CMS DUA will also prohibit the use of unsecured telecommunications to transmit such data, and will specify the circumstances under which such data must be stored and may be transmitted.

(b) A qualified entity must inform each beneficiary whose beneficiary identifiable data has been (or is reasonably believed to have been) inappropriately accessed, acquired, or disclosed in accordance with the DUA.

(c) Contractor(s) must report to the qualified entity whenever there is an incident where beneficiary identifiable data has been (or is reasonably believed to have been) inappropriately accessed, acquired, or disclosed.

(d) *Data use agreement between a qualified entity and an authorized user.* In addition to meeting the other requirements of this subpart, and as a precondition of selling or disclosing any combined data or any Medicare claims data (or any beneficiary-identifiable derivative data of either kind) and as a precondition of selling or disclosing non-public analyses that include individually identifiable beneficiary data, the qualified entity must enter a DUA (hereinafter the QE DUA) with the authorized user. Among other things laid out in this subpart, such QE DUA must contractually bind the authorized user (including any contractors or business associates described in the definition of authorized user) to the following:

(1)(i) The authorized user may be permitted to use such data and non-public analyses in a manner that a HIPAA Covered Entity could do under the following provisions:

(A) Activities falling under paragraph (1) of the definition of "health care operations" under 45 CFR 164.501: Quality improvement activities, including care coordination activities and efforts to track and manage medical costs; patient-safety activities; population-based activities such as

those aimed at improving patient safety, quality of care, or population health, including the development of new models of care, the development of means to expand coverage and improve access to healthcare, the development of means of reducing healthcare disparities, and the development or improvement of methods of payment or coverage policies.

(B) Activities falling under paragraph (2) of the definition of “health care operations” under 45 CFR 164.501: Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

(C) Activities that qualify as “fraud and abuse detection or compliance activities” under 45 CFR 164.506(c)(4)(ii).

(D) Activities that qualify as “treatment” under 45 CFR 164.501.

(ii) All other uses and disclosures of such data and/or such non-public analyses must be forbidden except to the extent a disclosure qualifies as a “required by law” disclosure as defined at 45 CFR 164.103.

(2) The authorized user is prohibited from using or disclosing the data or non-public analyses for marketing purposes as defined at § 401.703(s).

(3) The authorized user is required to ensure adequate privacy and security protection for such data and non-public analyses. At a minimum, regardless of whether the authorized user is a HIPAA covered entity, such protections of beneficiary identifiable data must be at least as protective as what is required of covered entities and their business associates regarding protected health information (PHI) under the HIPAA Privacy and Security Rules. In all cases, these requirements must be imposed for the life of such beneficiary identifiable data or non-public analyses and/or any derivative data, that is until all copies of such data or non-public analyses are returned or destroyed. Such duties must be written

in such a manner as to survive termination of the QE DUA, whether for cause or not.

(4) Except as provided for in paragraph (d)(5) of this section, the authorized user must be prohibited from re-disclosing or making public any such data or non-public analyses.

(5)(i) At the qualified entity’s discretion, it may permit an authorized user that is a provider as defined in § 401.703(b) or a supplier as defined in § 401.703(c), to re-disclose such data and non-public analyses as a covered entity will be permitted to disclose PHI under 45 CFR 164.506(c)(4)(i), under 45 CFR 164.506(c)(2), or under 45 CFR 164.502(e)(1).

(ii) All other uses and disclosures of such data and/or such non-public analyses is forbidden except to the extent a disclosure qualifies as a “required by law” disclosure.

(6) Authorized users who/that receive the beneficiary de-identified combined data or Medicare data as contemplated under § 401.718 are contractually prohibited from linking the beneficiary de-identified data to any other identifiable source of information, and must be contractually barred from attempting any other means of re-identifying any individual whose data is included in such data.

(7) The QE DUA must bind authorized user(s) to notifying the qualified entity of any violations of the QE DUA, and it must require the full cooperation of the authorized user in the qualified entity’s efforts to mitigate any harm that may result from such violations, or to comply with the breach provisions governing qualified entities under this subpart.

[76 FR 76567, Dec. 7, 2011, as amended at 81 FR 44479, July 7, 2016]

**§ 401.715 Selection and use of performance measures.**

(a) *Standard measures.* A standard measure is a measure that can be calculated in full or in part from claims data from other sources and the standardized extracts of Medicare Parts A and B claims, and Part D prescription drug event data and meets the following requirements:

(1) Meets one of the following criteria: