AKIN GUMP
STRAUSS HAUER & FELD LLP

Health Reform Alert

Proposed Rule on ACO Shared Savings Program Implicates HIPAA

April 22, 2011

On March 31, 2011, the Centers for Medicare & Medicaid Services (CMS) released a proposed rule to implement the Medicare Shared Savings Program, also known as the accountable care organization (ACO) provisions of the Patient Protection and Affordable Care Act (PPACA)[1]. Set forth below is an overview of how the proposed rule's data sharing provisions implicate the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations. Additional information about the proposed rule can be found at the Akin Gump Health Reform Resource Center. Comments on the rulemaking must be submitted to CMS by June 6, 2011.

Overview of How HIPAA Is Implicated by the ACO Proposed Rule

To further the Medicare Shared Savings Program's goals of improving health outcomes and achieving increased efficiency in the utilization of health care, CMS proposed sharing with ACOs both aggregate and individually identifiable Medicare beneficiary data. Importantly, individually identifiable beneficiary data shared with ACOs would be protected health information (PHI) for the purposes of HIPAA, and the players would be HIPAA "covered entities" or "business associates." HIPAA applies to covered entities, defined to include health care providers that engage in standard HIPAA transactions (such as claims processing), health plans and health care clearinghouses. HIPAA also extends to business associates, which are generally entities that create or receive PHI in order to perform a function or service for, or on behalf of, a covered entity.

To the extent CMS is a covered entity by virtue of the Medicare Fee-for-Service Program's status as a health plan (a status that CMS confirms in the proposed rule), its disclosure of such data would be subject to HIPAA. ACO providers and suppliers—which may include health care professionals in group practice arrangements, networks of individual professionals' practices, partnerships or joint ventures between certain hospitals and professionals, and certain hospitals employing professionals—that are HIPAA covered entities are also subject to the HIPAA privacy and security regulations in their use and re-disclosure of such data.

The HIPAA status of ACOs will vary from one entity to the next. CMS noted in the proposed rule that, in some cases, ACOs may be covered entities in their own right. For example, an ACO that is composed of physicians in a group practice may be considered a covered entity to the extent the group practice is a covered entity. In other situations, however, ACOs may be business associates of ACO participants that are covered entities. The proposed rule notes that in some cases, "based on their work on behalf of ACO participants and ACO providers/suppliers in conducting quality assessment and improvement activities, the ACOs will qualify as the business associates of their covered entity ACO participants and ACO providers/suppliers."[2] Accordingly, HIPAA-compliant business associate agreements (BAAs) may be required.

[1] *See* Medicare Shared Savings Program: Accountable Care Organizations and Medicare Program, 76 Fed. Reg. 19,528 (proposed Apr. 7, 2011) (to be codified at 42 C.F.R. pt. 425).
[2] 76 Fed. Reg. at 19,556.

www.twitter.com/akin_gump

While not discussed in the proposed rule, it seems that the "organized health care arrangement" (OHCA) concept under HIPAA could take on new significance in the ACO context. OHCAs are defined to include organized systems of health care in which more than one covered entity participates and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and engage in certain specific quality assessment and improvement activities. An OHCA designation would seemingly allow health care professionals and other covered entities participating in an ACO to share PHI with each other and with the ACO for health care operations purposes without entering into a BAA with the ACO. Similarly, the "affiliated covered entity" concept—under which covered entities that are legally separate but related (i.e., under common ownership or control) may designate themselves as a single affiliated covered entity for HIPAA privacy and security compliance purposes—could also take on new relevance.

Aggregate Data Sharing Under the ACO Proposed Rule

Under the proposed rule, CMS would provide ACOs with aggregate data on beneficiary use of health services in order to "monitor, understand, and manage its utilization and expenditure patterns, as well as to develop, target, and implement quality improvement programs and initiatives."[3] CMS requested comment on the kinds of aggregate data and the frequency of data reports that would be most helpful to ACOs in "coordinating care, improving health, and producing efficiencies."[4]

The proposed rule clarified that, by "aggregate data," CMS meant "data that omits the 18 identifiers listed at 45 C.F.R. 164.514(b)."[5] This approach will not necessarily create a truly de-identified data set, however, as defined for HIPAA purposes.[6] Under the HIPAA de-identification standard, unless the alternative statistical approach is applied, not only must the 18 identifiers be removed, but the covered entity must also not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.[7] While in large ACOs, such aggregate data would be, for all practical purposes, de-identified, there is some risk that aggregate data collected on beneficiaries in smaller ACOs may be attributed to particular patients or patient groups.

Individually Identifiable Data Sharing Under the ACO Proposed Rule

More significantly, the proposed rule would also allow ACOs access, upon request, to certain individually identifiable information about Medicare beneficiaries who would potentially be assigned to the ACO—including monthly claims data and basic identifiers (name, date of birth, Health Insurance Claim Number (HICN) and, potentially, gender). CMS noted that this approach would allow ACOs to improve care coordination and target inefficiencies by having some indication of the population involved.

All such individually identifiable beneficiary data is PHI under HIPAA and, as such, cannot be used or disclosed without the individual's specific written authorization (i.e., "opt-in") unless a HIPAA exception applies. CMS asserted that it is permitted to disclose such data for "health care operations" purposes under HIPAA, which include population-based activities relating to health improvement or health costs reduction, protocol development, case management and care coordination that ACOs are required to undertake.[8]

Despite this claim of legal authority to disclose the individually identifiable data, CMS proposed several additional protections. The proposed rule details certain certifications the ACO must make in requesting such data and also specifies that the ACO must enter into a Data Use Agreement with CMS (CMS Form-R-0235) in order to receive any

[3] *Id.* at 19,555.
[4] *Id.*
[5] *See id*. at 19,652 (to be codified at 42 C.F.R. § 425.19(b)).
[6] *See* 45 C.F.R. § 164.514(b)(1)-(2).
[7] *Id.*
[8] *See* 76 Fed. Reg. at 19,558.

beneficiary identifiable data. CMS also proposed allowing beneficiaries to "opt out" of having their individual claims data shared with the ACO, which could be challenging to implement. Importantly, the opt-out provision does not apply to the initial four data points CMS will provide to ACOs for individuals in the three-year base data set.[9]

HIPAA Action Items for ACOs and ACO Participants

The proposed rule's data sharing provisions, as well as other provisions requiring the establishment and use of electronic health records and other health information technology, would impose extra HIPAA-related compliance burdens on ACOs and ACO participants. ACOs will need to be formed with an eye toward HIPAA compliance.

It will be important to consider from the outset how data will flow into the ACO and among ACO participants so appropriate compliance steps can be taken. For instance, in addition to potentially needing to enter into new BAAs (with the ACO itself) and support the new opt-out mechanism, ACO participants would likely need to update their HIPAA privacy and security policies to ensure that appropriate safeguards and structures are in place. Forms, such as the notice of privacy practices, would also need to be revisited. ACOs that are covered entities would need to complete similar updates, and, in light of the changes to the HIPAA regime enacted through the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), ACOs that are business associates would need to address their own HIPAA compliance. Overall, while the HIPAA implications of the data sharing provisions of the ACO proposed rule warrant careful attention, many of the issues raised can be addressed through existing HIPAA compliance mechanisms.

CONTACT INFORMATION

If you have any questions concerning this alert, please contact —

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
202.887.4220
Washington, D.C.

Anna R. Dolinsky
adolinsky@akingump.com
202.887.4504
Washington, D.C.

Kristen Henderson
khenderson@akingump.com
202.887.4587
Washington, D.C.

[9] *See id.* at 19,653 (to be codified at 42 C.F.R. § 425.19(g)).