Connecting Healthcare with Legal Excellence℠

Health Law Diagnosis

PATIENT CONSENT AND OPT-OUT PROVISIOSN UNDER THE PROPOSED RULEMAKING AND FINAL RULE FOR ACCOUNTABLE CARE ORGANIZATIONS

On March 30, 2011, the Department of Health and Human Services (HHS) released the Notice of Proposed Rulemaking (the "Proposed Rule") for the Medicare Shared Savings Program and Accountable Care Organizations (ACOs). A Joint Policy Statement was also released by the Office of the Inspector General (OIG) and Federal Trade Commission (FTC) providing guidance for ACOs in operating under constraints of federal antitrust laws. The Proposed Rule sets forth proposed regulations for the structure and governance of ACOs. It made clear that CMS did not intend to *require* an ACO be formed as a separate legal entity but required any entity seeking to become an ACO be a legally recognized entity under state law and have a taxpayer identification number (TIN) in addition to meeting additional requirements. Each qualifying ACO entity would need to commit to a minimum of ***three-years*** through ***agreement with CMS*** and be governed by a variety of ACO providers and suppliers (i.e., ACO Participants) and Medicare beneficiaries or their representatives.

Of particular interest to patient privacy, the Proposed Rule would ***authorize key data sharing*** between CMS and an ACO. In particular, four categories of data could potentially be shared:

- **Aggregated Data** (*presumably* de-identified), both from ACOs and non-ACO entities, on beneficiary use of health care services, which would include *aggregated metrics on assigned beneficiary populations and beneficiary utilization data* at the start of the agreement period based on historical data used to calculate the benchmark, and quarterly aggregate data reports;

- **Personal Identifiers**, which would include the beneficiaries' names, date of birth, gender and Medicare ID, for all historically assigned ACO patients included in the aggregate data reports;

- **Personally Identifiable Claims Data**, which would include procedure code, diagnosis code, beneficiary ID, date of birth, gender, and, if applicable, also the date of death, claim ID, from and thru dates of service, provider or supplier ID and claim payment type, but only on a monthly basis upon a participating ACOs request; and

- **Prescription Claims Data**, regarding prescription drug use, which could potentially include beneficiary ID, prescriber ID, drug service data, drug product service ID, and indication of the drug is on the formulary.

CMS emphasized in the Preamble to the Proposed Rule the importance of sharing these forms of data in order provide more complete information for the services provided or coordinated for the ACO beneficiary populations, better achieve improvements in the quality of care and gain a better understanding of the population served while lowering the growth in health care costs. Although ***beneficiaries would be able to "opt-out" of certain data sharing,*** other data sharing would occur *without the patient's consent*. CMS deliberately chose to proceed with an opt-out approach, given its concerns for beneficiary participation and ACO Participant administrative burdens. In the Preamble to the Proposed Rule, it noted that,

> "*An opt-out approach is used successfully in most systems of electronic exchange of information because it is significantly less burdensome on consumers and providers while still providing an opportunity for caregivers to engage with patients to promote trust and permitting patients to exercise control over their data*."[1]

CMS has proposed to develop a communications plan in order to communicate key information to beneficiaries about the Shared Savings Program and ACOs, as well as their right to opt-out of the data sharing portion of the Program. CMS explicitly notes that the decision to opt-out in no way effects use of beneficiaries' data or assignment to the ACO for purposes of determining calculations such as ACO benchmarks, per capita costs, or quality performance.

The Final Rule for ACOs was released in October 2011 after careful consideration of the substantial comments received from the public and private sectors. Significant changes included:

- Shared savings model only (i.e., *participating providers can join a three-year shared-savings version only rather than bear risk by year three*);
- Far fewer performance measures (*reduced nearly in half*);
- More flexibility in governance and structural requirements (i.e., *Meaningful Use relegated to a performance measure instead of requirement*); and
- Revised approach to assigning beneficiaries to the ACOs.

Although substantially more expansive than the Proposed Rule in many respects, and with many revisions in response to comments received on the originally proposed requirements and provisions, the Final Rule with regard to ***data sharing and beneficiary opt-out remained substantially unchanged.***

[1] *See* 76 Fed Reg. 19560 (2011).

Data Sharing *Without* Opportunity to Opt-Out

Sharing Aggregate Data

CMS proposed to permit the sharing of aggregate and de-identified data concerning beneficiary use of health services. An ACO would then use such aggregated data reports concerning its assigned or potentially assigned beneficiary population 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."[2] The Proposed Rule gives the following ***examples of uses of aggregate data***:

- Data showing high rate of hospital readmissions could highlight need for action to improve discharge coordination among physicians, hospitals and post-acute care providers, or improve access to primary care clinics;

- Data showing beneficiaries were not filling prescriptions could lead to interventions designed to assess and develop strategies to overcome difficulties in filling prescriptions;

- Data showing relatively high incidence of certain types of procedures relative to national benchmarks could lead to exploration and examination of appropriateness of ACO Participants' practice patterns by using provider-level data.

Because the aggregated data would be ***de-identified***, HIPAA and the federal Privacy Act would not be implicated in the sharing of such information without patient authorization. Likewise, state confidentiality laws likely would also not be implicated. The Final ACO Rule adopted these provisions as set forth in the Proposed Rule with very little change.

Identifying Historically Assigned Beneficiaries

CMS also proposed to make available limited beneficiary identifiable data at the beginning of the first performance year and in connection with quarterly aggregated data reports. In the Proposed Rule, it stated, "We believe the ACO would benefit from understanding which of their fee-for-service beneficiaries were used to generate the aggregated data reports."[3] Accordingly, the following information would be disclosed by CMS (referred to hereinafter as the "Beneficiary Identifiers"):

- Beneficiary **name**;

- Beneficiary **date of birth**;

- Beneficiary **sex**; and

- Beneficiary Health Insurance Claim Number (**HICN**).

[2] 76 Fed Reg at 19555.
[3] 76 Fed Reg at 19555.

ACO providers could use this information to identify their beneficiaries, review records, and identify any care processes that may be in need of change, such as inability to receive timely clinic appointments resulting in a trip to the emergency room for a particular patient. Second, given that a high percentage of historically assigned patients in the PGP demonstration[4] continued to receive care from the ACO Participants, knowing individuals who have been assigned in the past would help identify individuals in need of improved care coordination strategies in the future.

Nevertheless, CMS noted concerns with sharing this information, in particular individually-identifiable health information. The Affordable Care Act at § 1106 bars disclosure of information collected under the Act without consent unless a law permits for the disclosure. However, CMS takes the position that the HIPAA Privacy Rule permits disclosure for purposes of sharing Medicare Part A and Part B claims data with ACOs participating in the Shared Savings Program".[5] In both the Proposed and Final ACO Rules, CMS states generally that "[W]e have the legal authority within the limits described previously to share Medicare claims data with ACOs without the consent of the patients..."[6]

In addressing the release of claims data for performance measurements in a separate rule, CMS also additionally notes that the agency "[i]s merely providing data to qualified entities in accordance with the mandate in the Affordable Care Act, and, as such, its disclosure of protected health information is permitted by the HIPAA Privacy Rule as "required by law" (45 CFR 164.512(a))."[7] However, it is also noted that CMS does not have the statutory authority to require qualified entities to release their *own* claims data to providers or suppliers upon their request, but to the extent the qualified entities have the statutory authority to do so, they are encouraged to.[8] The ACO rules also interestingly do not actually address **Part D data** in the context of HIPAA specifically, but this may be because the data proposed to be shared would not include any PHI. However, CMS does note that **state law would govern** the privacy and security of any Part D Medicare data once received pursuant to the rule.

HIPAA "Health Care Operations"

Under HIPAA, ACOs would be considered either HIPAA covered entities, to the extent they would be a health care provider conducting such transactions, or HIPAA Business Associates (HIPAA BA) based on their work on behalf of ACO Participants and providers/suppliers in conducting quality assessment and improvement activities. The Medicare FFS program itself would also be considered a covered entity as a "health plan" function of HHS. As set forth in the Preamble to the Proposed Rule, disclosure of the four Beneficiary Identifiers would be permitted by HIPAA as "health care operations."

Under the HIPAA health care operations provisions, a covered entity, or a business associate on its behalf, is not prohibited (by HIPAA) from disclosing PHI to another covered

[4] The PGP (Physician Group Practice) demonstration was conducted by CMS for a period of 5 years with a select group of physician group practices, and essentially tested the ACO framework by using a hybrid payment structure of regular Medicare FFS and opportunity to earn bonus payments (shared savings).

[5] See 76 Fed Reg 19558 (2011).

[6] See 76 Fed Reg 19558; and 76 Fed Reg 67489.

[7] See Final Rule, 76 Fed Reg 76553.

[8] See Final Rule, 76 Fed Reg 76558.

entity for the recipient's health care operations purposes where: (1) both covered entities have or had a relationship with the individual, (2) the PHI pertains to that relationship and (3) the recipient will use the PHI for certain health care operations, as applicable to ACOs here, those related to population-based activities; i.e., improving health, reducing health costs, protocol development, case management and care coordination (45 CFR 164.501). The Proposed Rule states that this definition of health care operation covering population activities is "*extensive enough to cover the uses we would expect an ACO to make of the identifying data elements for the historically assigned patients*."[9]

The Proposed Rule as well as the Final ACO Rule also noted that CMS believes that, while an individual's authorization is required before disclosing PHI for marketing purposes, both ACOs acting as covered entities and those acting as business associates ***will*** also be able to use the four Beneficiary Identifiers to "*communicate with individuals on the list to describe available services and for case management and care coordination purposes under the exceptions to the definition of marketing under [HIPAA*]."[10] Additionally, CMS noted that sharing the four Beneficiary Identifiers would constitute the "minimum data necessary" to accomplish the intended purpose of the use, disclosure or request, as required by HIPAA.

Privacy Act "Routine Uses"

The Federal Privacy Act generally requires an individual's authorization prior to any agency disclosing an individual's information from a "system of records." An exception to this is "routine uses." For routine uses, an agency may disclose records and information outside of the agency where the disclosure would be compatible with the purpose for which the data was collected by the agency. All routine uses, however, must be published in the Federal Register concerning the applicable system of records that describes the purpose of the disclosure and to whom the disclosure will be made. CMS notes that it believes that the proposed disclosures of the four Beneficiary Identifiers would be consistent with the purpose for which the data was collected and provided appropriate publication (in the Federal Register) of the "routine use" is put in place prior to any disclosures being made.

Data Sharing *With* Opportunity to Opt-Out

Sharing Identifiable Data (Parts A and B) and Prescription Data (Part D)

The Proposed Rule *would permit ACOs to* ***request more complete data*** in addition to the de-identified aggregate data that would be made available to them. CMS proposed to share claims data with the ACOs in order to assist them in improving care for individuals, improving health of their population, and reducing the growth in expenditures for their assigned beneficiary population. ACOs would be permitted to request claims data from CMS on a monthly basis, *in compliance with applicable laws*, in standardized data sets about those beneficiaries currently being served by the ACO Participants and providers/suppliers. However, information subject to additional legal protection, such as under 42 CFR Part 2 concerning alcohol or drug use/abuse treatment, could not be released without the beneficiary's specific authorization.

[9] 76 Fed Reg 19556.
[10] 76 Fed Reg 19556.

The data sets would be limited to beneficiaries who have received services from a primary care physician participating in the ACO during the performance year and who have not "opted out" of having CMS share their claims data with the ACO. The content of the data would also be limited to the "minimum necessary" for the ACO to effectively coordinate care of its patient population. ACOs would be required to explain their intended use of the data for evaluating ACO Participant performance, quality assessment and improvement activities, and conduct population-based activities to improve the health of the assigned beneficiary population. Data proposed to be shared could potentially include:

Part A and B:

- Procedure codes;
- Diagnosis codes;
- Beneficiary ID;
- Date of birth;
- Gender; and
- (if applicable) date of death, claim ID, from and thru dates of service, provider or supplier ID, and claim payment type.

Part D:

- Beneficiary ID;
- Prescriber ID;
- Drug service date;
- Drug product service ID; and
- Indication if drug is on the formulary.

Furthermore, a **Data Use Agreement** (DUA) would need to be entered into by the ACOs prior to receipt of any beneficiary identifiable claims data. The DUA would prohibit the ACO from sharing the Medicare claims data with anyone outside the ACO, as well as require the ACO agree not to use or disclose the claims data obtained under the DUA in any manner in which a HIPAA Covered entity could not without violating the HIPAA Privacy Rule. Compliance with the DUA would be a condition of the ACO's participation in the Shared Savings Program.

CMS specifically notes that the disclosures of claims data would be permitted as health care operations. As discussed previously in this summary, a covered entity may disclose PHI to another covered entity for the recipient's health care operations if they both have or had a relationship with the individual, the records pertain to that relationship, and the records will be used for a health care operation function meeting one of the first two paragraphs in the definition of health care operation under HIPAA. Therefore, where disclosed for population activities, evaluating a provider's or supplier's performance, quality assessment and improvement activities, HIPAA would not require the individual's authorization.

Patients' Right to "Opt-Out"

Although CMS explicitly states that it has the authority to share Medicare Claims Data without consent with the ACOs, and believes the data would be a valuable tool for ACOs in "evaluating the performance of ACO participants and ACO providers/suppliers, conducting quality assessment and improvement activities," the agency states that it "*nonetheless believe(s) that **beneficiaries should be notified of, and have meaningful control over** who, has access to their personal health information for purposes of the Shared Savings Program*."[11] While, under the ACO Rule patients would not be able to opt-out of having the four previously discussed Beneficiary Identifiers shared with the ACOs or de-identified aggregated data reports shared, CMS *would* allow the patients to opt-out of having Claims Data shared with the ACOs.

[11] 76 FR 19559; See also 76 FR 67849.

ACOs would therefore be required to ***not only*** notify beneficiaries that their providers or suppliers are participating in an ACO, but **also inform beneficiaries that they would be able to request claims data about them if they do not opt-out.** CMS specifically notes that a beneficiary choosing to opt-out is only opting out of the data sharing portion of the program. Under the ACO rule, an opt-out would not affect use of beneficiaries' data or assignment for other purposes such as determining ACO benchmarks, per capita costs, quality performance, or performance year per capita expenditures.

The Final ACO Rule adopted these provisions of the Proposed Rule, despite comments that allowing beneficiaries to opt-out would have a negative impact on the operation of ACOs and that it ran "counter to the goal of coordinated care", making it nearly impossible for ACOs to succeed. However, CMS reiterated that while it had the authority to exchange data without requiring an opt-out opportunity, it believes ***beneficiaries should be notified*** of their providers' participation in an ACO and have some control over who has access to their personal health information.[12]

Data Sharing Between Participants and with Other ACO Providers/Suppliers

Neither the Proposed Rule or Final ACO Rule directly address the extent to which ACOs may share information between their Participants, providers and suppliers or with other third parties. The focus, rather, is on the extent to which ***CMS*** may share claims and other beneficiary identifiable data ***with the ACOs*** within federal privacy laws, and vice versa. As such, HIPAA and other federal and state privacy and security laws and regulations will still affect the extent to which ACOs may use and disclose beneficiary identifiable information that they independently collect, receive and/or maintain.

As noted by CMS in the Final Rule, "ACOs must comply with the limitations on use and disclosure that are imposed by HIPAA, the applicable DUA, and the ACO program's statutory and regulatory requirements."[13] Additionally, CMS stated, "The HIPAA Privacy and Security Rules will provide *added* protections (and enforcement mechanisms) outside of the ACO program requirements."[14] ACOs monitoring protocols would also help protect beneficiary privacy interests and penalize ACOs misusing data.[15]

As discussed previously, HIPAA may apply to ACOs, their Participants, providers and suppliers as either covered entities or business associates. Therefore, HIPAA BA Agreements must be entered into as applicable between the ACOs, their Participants and providers/suppliers. Furthermore, a written DUA (Data Use Agreement) is required for CMS to disclose data to the ACO. Through the DUA which each ACO must enter into prior to receiving any data from CMS, ACO Participants, providers and suppliers are also obligated not to disclose any claims information *outside of the ACO* (unless such entity co-signed the DUA with the ACO) as well as not use or disclose any of the information unless it would be permitted by the covered entity to do so under HIPAA. Likewise, federal substance abuse regulations and State law may restrict disclosure of certain information, such as alcohol/drug use and abuse

[12] 76 FR 67849.
[13] 76 Fed Reg 67846.
[14] 76 Fed Reg 67848.
[15] Id.

information and HIV/AIDS related information, without obtaining patient authorization even if HIPAA itself would not prohibit disclosure of such information.

Therefore, HIPAA will apply both to the disclosure of information by CMS to the ACOs and to their subsequent use and disclosure of such information, as well as information independently obtained by the ACOs and their Participants and providers/suppliers. Once claims data is received by an ACO, it may only release the data to entities participating in the ACO and providers/suppliers of the ACO, and for only those uses and disclosures as would otherwise be permitted (i.e., not prohibited) by HIPAA. For all claims and other data independently maintained or received by the ACOs, ACOs would also be permitted to use and disclose the information as would be permitted (i.e., not prohibited) by HIPAA, within the restrictions of any applicable state laws, and not necessarily only within the ACO structure. As explicitly noted in the Final ACO Rule, even where beneficiaries opt-out of having their claims data shared, this would not prohibit medical information being shared among physicians as allowed under HIPAA and other applicable state and federal laws.

* * * *

For more information, please contact:

Krystyna Monticello, Esq.
Partner at Oscislawski LLC
tel: 609-385-0833, ext. 2
kmonticello@oscislaw.com

OR

Helen Oscislawski, Esq.
Principal at Oscislawski LLC
tel: 609-385-0833, ext. 1
helen@oscislaw.com

Attorneys at Oscislawski LLC is a health law firm with its main office located in Princeton, New Jersey but a nationwide reputation for experience with and understanding of federal and state privacy and security laws, as well as electronic health information exchange, health information technology, and managing health data breaches. Our attorneys also advise clients on wide-range of other legal issues. For more information about our firm visit www.oscislaw.com. ***For excellent compliance information, tools and solutions, please also visit our affiliated blog & resource website*** *www.legalhie.com.*