Changes to Stark Law Special Compensation Rules for Group Practices Go into Effect on January 1, 2022

The final rules regarding special compensation under **42 U.S.C. § 1395nn**, the Physician Self-Referral or Stark Law, go into effect on January 1, 2022 and will require many physician group practices to modify their compensation methodologies, specifically the pooling and distribution of profits for the provision **designated health services** ("DHS").

Under the **current regulations**, a physician in a group practice that relies on the in-office ancillary services exception can be paid a share of overall group profits, so long as that share is determined in a way that is not "directly related to the volume or value of referrals of DHS by the physician." The same is true of productivity bonuses based on services that a physician has performed. "A physician in the group practice may be paid a productivity bonus based on services that he or she has personally performed, or services 'incident to' such personally performed services, or both, provided that the bonus is not determined in any manner that is directly related to the volume or value of referrals of DHS by the physician (except that the bonus may directly relate to the volume or value of DHS referrals by the physician if the referrals are for services 'incident to' the physician's personally performed services)."

This provision had previously been interpreted to allow "split pool" profit-sharing plans that create pools of DHS-derived profits for different services, in which only certain physicians benefit from certain profit pools.

Effective January 1, 2022, split pooling is no longer permitted. In the **final regulation**, which modifies the special compensation rules under 42 C.F.R. §411.352(i), CMS clarifies that "if a group practice wishes to pay shares of overall profits to any of its physicians, it must first aggregate: (1) The entire profits from the entire group; or (2) the entire profits from any component of the group that consists of at least five physicians. Once aggregated, the group practice may choose to retain some of the profits or distribute all of the profits through shares of overall profits paid to its physicians." Therefore, although a group practice may employ different profit distribution methods for the provision of DHS for each component of the group practice that consists of five or more physicians, the group practice must employ the same method for distributing overall profits to every physician within such a component. It is important to note that although CMS limited the general definition of DHS to "only DHS payable in whole or in part by Medicare" in § 411.351, "overall profits" for the purpose of the special compensation rules for group practices continues to include "the group's entire profits derived from DHS payable to Medicare or Medicaid."

Group practices that currently employ the split pool compensation structure for physicians and rely on the in-office ancillary services exception will need to modify their compensation structures to

comply with this clarification.

Reality Check: FDA Draft Guidance Outlines Considerations for the Use of Real-World Data and Real-World Evidence to Support Regulatory Decision-Making for Drugs and Biological Products

 Last week the FDA issued another draft guidance in its series of recent guidance documents setting forth the agency's views regarding the generation and use of Real-World Data (RWD) and Real-World Evidence (RWE) for prescription drugs and biological products. (see our **recent post** on FDA's draft guidance relating to registries).

This latest draft guidance, **Considerations for the Use of Real-World Data and Real-World Evidence to Support Regulatory Decision-Making for Drug and Biological Products**, clarifies the agency's expectations for sponsors submitting new drug applications (NDAs) or biologics license applications (BLAs) with studies using Real-World Data (RWD) to support the safety or effectiveness of drugs or biological products, when such studies are not subject to FDA's investigational new drug (IND) application requirements under **21 CFR Part 312**. The draft guidance focuses on non-interventional (*a.k.a.* observational) studies, in which patients receive a drug during routine medical practice, according to a medical provider's clinical judgment and based on patient characteristics, rather than via assignment to a study arm and according to a clinical trial protocol.

Key considerations outlined in the guidance:

- *Sponsors designing a non-interventional study to support a marketing application should engage early with the relevant FDA review division* (e.g., through a Type C meeting) and be prepared to submit draft protocols and SAPs for FDA feedback *before* conducting the study analyses.

- *To assure the FDA that the results of a non-interventional study were not skewed to favor a particular conclusion,* sponsors should provide evidence that the non-interventional study protocol and statistical analysis plan were finalized *prior* to reviewing outcome data and *before* performing prespecified analyses. Sponsors should provide a justification for selecting relevant data sources and generate audit trails in their datasets. FDA also recommends that sponsors post their non-interventional study protocols on a publicly available website, such as **ClinicalTrials.gov**.

- *Sponsors must be able to submit patient-level data from the RWD.* Where a third party owns or controls the RWD, sponsors should have agreements with such parties to ensure that patient-level data and source data to verify the RWD can be provided to the FDA for inspection, as applicable. Sponsors should have well-documented programming codes and algorithms that would allow the FDA to replicate the study analysis using the same dataset and analytic approach.

- *Non-interventional studies should be monitored*. The FDA advises sponsors to use a risk-based quality management approach, with a focus on preventing or mitigating important and/or likely risks to study quality. If a non-interventional study does not include any activities or procedures involving patients, monitoring can focus on assuring the data integrity of the RWD, from extraction to analysis to reporting of results. When a non-interventional study protocol includes ancillary activities or procedures, sponsors should exercise appropriate oversight of processes critical to human subject protection.

- *Adverse events that a sponsor becomes aware of through a non-interventional study must be submitted in accordance with postmarketing safety reporting regulations*. However, the agency acknowledges that if a sponsor is conducting a non-interventional study that appropriately utilizes only a subset of a larger dataset, the sponsor will not have to search the entirety of the dataset for adverse events.

- *Sponsors should take responsibility for all activities related to the design, conduct and oversight of a non-interventional study that is being submitted for regulatory review*. This includes selecting qualified researchers, ensuring the study is conducted in accordance with the protocol, maintaining and retaining adequate study records, and maintaining an electronic system to manage RWD that complies with **21 CFR Part 11**. Where a sponsor engages third parties to perform certain study-related tasks, the responsibilities of each organization should be documented and made readily available to the FDA upon request.

Comments on the guidance should be submitted to the docket by March 9, 2022.

---

3 Key Considerations for Promoting Transparency for AI/ML-Enabled Medical Devices

Today, developers of innovative medical devices are increasingly utilizing artificial intelligence (AI) and machine learning (ML) technologies to derive important insights with the promise of transforming the delivery of healthcare. Yet, concerns regarding the transparency of AI/ML-enabled devices, or the degree to which information about such devices is communicated to stakeholders, threatens not only perceptions as to the safety and effectiveness of such devices by regulators, but also trust in such technologies from patients and healthcare providers alike.

Read the full **article** written by **Steven Tjoe** in *PM360 Magazine*.

Visit the **Goodwin on Medtech hub** to stay informed on important developments affecting medtech innovators and investors.

DOJ Announces New Initiative to Use False Claims Act to Enforce Compliance with Data Privacy and Security Laws and Contract Requirements

The Department of Justice recently announced the launch of its new Civil Cyber-Fraud Initiative (the "Initiative") which intends to use the False Claims Act to pursue "cybersecurity-related fraud by government contractors and grant recipients."

Specifically, the Initiative will target those who:

1. knowingly provide deficient cybersecurity products or services,
2. knowingly misrepresenting their cybersecurity practices or protocols, or
3. knowingly violate obligations to monitor and report cybersecurity incidents and breaches.

This new initiative significantly expands the potential liability of federal contractors and healthcare provider that participate in federal healthcare programs related to data privacy and cybersecurity issues.

False Claims Act

The False Claims Act broadly prohibits anyone from, among other things, knowingly presenting, or "causing to be presented" a false claim for payment if the claim will be paid directly or indirectly by the federal government. The False Claims Act is the government's main enforcement tool for fighting healthcare fraud, with over $2.2 billion recovered in 2020. Penalties for False Claims Act violations include three times the actual damages sustained by the government, mandatory civil penalties of between $11,181 and $22,363 for each separate false claim, and attorneys' fees and costs. Further,

the False Claims Act allows whistleblowers to bring lawsuits on behalf of the federal government. Also known as a "qui tam" realtor, a whistleblower who brings a successful *qui tam* action can receive 15 to 30 percent of the damages the government recovers from the defendants. The ability for an individual within one's own organization to raise flags with the federal government under the False Claims Act especially heightens risk.

HIPAA

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), "covered entities" and their "business associates" are subject to certain obligations and limitation related to their use and disclosure of "protected health information" ("PHI"). Covered entities are health care providers, health plans and health care clearing houses that transmit any information in an electronic form in connection with a transaction for which HHS has adopted standards. A business associate is a person or entity that performs certain services for or functions on behalf of the covered entity that involve the use or disclosure of PHI. Finally, PHI is any individually identifiable information, including demographic data, that relates to an individual's past, present or future health or payment for the provision of healthcare.

The obligations imposed on covered entities and business associates under HIPAA include maintaining and following specific privacy and security policies and procedures regarding access to, use, processing, transfer, storage, and disclosure of PHI and implementing physical, technical, and administrative safeguards to protect the privacy and security of PHI. In addition, covered entities are required to notify affected individuals, the Department of Health and Human Services, and, for certain larger breaches, the media of data breaches. Similarly, business associates are required to notify covered entities of data breaches.

Implications

The goal of holding accountable those who "knowingly provide deficient cybersecurity products or services, knowingly misrepresent their cybersecurity practices or protocols, or knowingly violate obligations to monitor and report cybersecurity incidents and breaches" presents particular risk for covered entities and their business associates.

For example, consider a revenue cycle management ("RCM") company that submits claims on behalf of a healthcare provider (including claims to government payors) that experiences a security incident, conducts a HIPAA risk assessment, and shares that assessment with the Covered Entity customer who determines the RCM company did not implement the necessary physical, technical and administrative safeguards required under HIPAA. Could the customer, the government, or a whistleblower allege that the RCM company knowingly misrepresented its cybersecurity practices or protocols and thereby caused the submission of false claims?

Further, consider an electronic health records company ("EHR") that is certified by the Office of the National Coordinator who experiences a breach of unsecured PHI, conducts a HIPAA risk assessment and determines it is not obligated to report the breach based on a low risk of compromise in accordance with 45 C.F.R. 164.402. Could the government or a whistleblower allege that the EHR company failed to report a breach and thus caused the submission of false claims by healthcare providers that use its EHR and are able to avoid reductions in Medicare reimbursement by using a certified EHR?

False Claims Act cases are commonly pursued under what is known as the "false certification theory". A claim is considered false when a claimant "certifies compliance with a statute or regulation as a condition to governmental payment." The false certification theory considers a

claimant's *request* for payment as "implied certification" of compliance with said statutes or regulations. Despite the broad implications of the false certification theory, there is some check on the ability of the government or a whistleblower to bring cases on failure to comply with HIPAA through what is known as the materiality requirement under the False Claims Act. In *Universal Health Services v. United States ex rel. Escobar*, the U.S. Supreme Court held that the government and whistleblowers bear the burden of proving the "rigorous and demanding" materiality requirement under the False Claims Act. The Supreme Court further stated that the False Claims Act is "is not a means of imposing treble damages and other penalties for *insignificant* regulatory or contractual violations." Accordingly, the government and whistleblowers must demonstrate that allegedly insufficient technical safeguards or that an alleged failure to report a breach are actually *material* to the government's payment decision.

The potential use of the False Claims Act to enforce HIPAA compliance may also change how due diligence is conducted on covered entities who bill government payors and their and business associates. While security incidents are common, the potential for liability under the False Claims Act related to such an incident increases the importance of conducting thorough diligence related to such incidents. The importance of conducting due diligence on a seller's compliance with HIPAA's requirements related to administrative, technical, and physical safeguards is also magnified by the potential for liability under the False Claims Act for failure to comply with those requirements. The risk related to conducting a risk assessment related to a data breach is similarly increased and such assessments should be scrutinized carefully in due diligence.

It's Starting to Register: FDA Draft Guidance Addresses Use of Registries to Support Regulatory Decision-Making for Drugs & Biological Products

Showing no signs of food coma, the FDA issued **draft guidance** on the Monday following the Thanksgiving holiday weekend that outlines considerations for sponsors proposing to design a registry or use an existing registry to support regulatory decision-making about a drug's effectiveness or safety. This draft guidance represents the Agency's latest response to the mandate in the 21st Century Cures Act to issue guidance on the use of real world evidence in regulatory decision-making, and expands on the **Framework for FDA's Real-World Evidence Program** from December 2018.

The draft guidance, ***Real-World Data: Assessing Registries to Support Regulatory Decision-***

Making for Drug and Biological Products, defines a registry as "an organized system that collects clinical and other data in a standardized format for a population defined by a particular disease, condition, or exposure," and identifies three general categories of registries: disease registries, health service registries, and product registries.

Given the range of registry types, FDA notes that registry data can have varying degrees of suitability for use in a regulatory context depending on several factors, including how the data are intended to be used for regulatory purposes, the patient population enrolled, the data collected, and how registry datasets are created, maintained, curated, and analyzed. FDA advises sponsors to be mindful of both the strengths and limitations of using registries as a source of data to support regulatory decision-making. In general, the draft guidance advises that (i) a registry that captures objective endpoints, such as death or hospitalization, is more likely to be suitable to support regulatory decision-making than a registry that collects subjective endpoints, such as pain; and (ii) a registry that is specifically designed to answer a particular research question is more likely to be useful to support regulatory decision-making than a registry that was designed for a different purpose.

At the same time, the Agency acknowledges that an existing registry can be used to collect data for purposes other than those originally intended, and that leveraging an existing registry's infrastructure to support multiple purposes can be efficient. Therefore, the draft guidance describes factors sponsors can use to assess the **relevance** and **reliability** of a registry's data to determine whether the registry data may be fit-for-use.

When determining **relevance** of registry data, the draft guidance advises sponsors to consider, among other things, whether the data elements captured by the registry are sufficient given the intended use or uses of the registry (e.g., external control arm vs. a tool to enroll participants in an interventional study) and whether the methods involved in patient selection may have impacted the representativeness of the population in the registry.

When assessing the **reliability** of registry data, the draft guidance advises sponsors to assure the registry has appropriate governance measures in place to help ensure the registry can meet its objectives, such as processes and procedures governing the operation of the registry, adequate training of staff, and other recommended practices including:

- Defined processes and procedures for data collection, management and storage;
- A data dictionary and rules for validation of queries and edit checks of registry data;
- Conformance with **21 CFR part 11**, as applicable, including access controls and audit trails; and
- Adherence to applicable human subject protection requirements, including safeguarding the privacy of patient health information.

The draft guidance specifically recommends that sponsors interested in using a registry to support a regulatory decision should meet with the relevant FDA review division (e.g., through a Type C meeting), *before* conducting a study that will include registry data. Sponsors also should be prepared to submit protocols and statistical analysis plans for FDA feedback prior to conducting a study that includes data from registries.

Comments on the guidance should be submitted to the docket by February 28, 2022.