September 5, 2013

Ms. Marilyn Tavenner
Administrator
Centers for Medicare and Medicaid Services
Department of Health and Human Services
200 Independence Ave., SW
Office 341D-05
Washington, D.C. 20201

Via e-mail: Physician_Data_Comments@cms.hhs.gov

Attn: *Physician Data Comments*

Dear Ms. Tavenner:

We respectfully submit this letter, on behalf of CDT and the signatories below, in response to the Centers for Medicare and Medicaid Services (CMS)' request for public comments on the release of Medicare physician data.

The Center for Democracy & Technology ("CDT") is a non-profit Internet and technology advocacy organization that promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education and litigation, as well as through the development of industry best practices and technology standards. Recognizing that a networked health care system can lead to improved health care quality, reduced costs, and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

CDT is frequently relied on for sound policy advice regarding the challenges to health privacy and security presented by health information technology (health IT) initiatives. We have testified before the U.S. Congress five times since 2008 on the privacy and security issues raised by health IT, and we chair the privacy

and security policy working group of the federal Health IT Policy Committee (called the "Tiger Team").

We support CMS' efforts to make Medicare data available to serve the public interest; our comments below address the privacy and security issues raised in the Request for Comment.

Physician Privacy Interest

In *Florida Medical Ass'n Inc. v. Department of Health, Educ. & Welfare,*[1] a Florida federal district court lifted the 1979 injunction prohibiting the Department of Health, Education and Welfare – now the Department of Health and Human Services (HHS) – from releasing physician-level Medicare payment data. However, the vacatur of the injunction does not mean this information is now automatically available to anyone who requests it. Instead, the Centers for Medicare and Medicaid Services (CMS) must establish policies to determine the circumstances when the public interest in this information outweighs any interests the physicians may have in preventing disclosure of this information.

We support CMS' efforts to establish policies and a process for determining when this information will be released. We urge HHS to continue to evaluate requests for this information based on whether the information will be used to further the public's interest. Consumers and patients suffer the most from a health care system that costs too much and too frequently delivers poor-to-mediocre quality care. Medicare data can be key to gaining a better understanding of these trends and how to reverse them. Taxes from consumers and patients substantially fund the Medicare program; consequently, data generated by this program should be available for uses that have the potential to serve their interests. For example, CMS should view favorably requests for Medicare payment data where the recipient commits to sharing analyses of payment data with the general public.

CMS should take care not to overstate the "privacy" interests of physicians. The behavior of physicians and other health care professionals is routinely scrutinized by federal and state regulators, accrediting organizations, licensing boards, and health care plans, among others. A broadly recognized privacy interest in physician-level Medicare data could have implications for multiple important initiatives, including quality measurement and public reporting, as well as comparative effectiveness research, which are critical to reform of our health care system. At the same time, we recognize that this data could be used to discriminate against professionals or in ways that have a negative impact on their operations. CMS does have an obligation to carefully review requests for this information, balancing the importance of advancing the interests of the public against the interests of physicians and other professionals in this data. We urge

[1] 2013 WL 2382270 (M.D. Fla. May 31, 2013)

CMS to make public all decisions made regarding requests to release claims data, as transparency about uses of health information is a key principle of Fair Information Practices.

In implementing a new process for reviewing requests for Medicare data, CMS must take care to apply review criteria consistently, and not establish per se barriers to access. In *Sorrell et al. v. IMS Health Inc. et al.,*[2] the Supreme Court struck down state limitations on health information access that barred access based on type of requester (pharmaceutical manufacturers) and the specific purpose of the request (marketing). The standards that CMS will apply to requests for Medicare data, and the process for requesting data, should be transparent to the public. Appeals of CMS decisions can proceed under the Administrative Procedure Act (APA).

Protecting Patient Privacy

We are pleased that CMS does not intend to disclose, "…any information that could directly or indirectly reveal patient-identifiable information." However, we urge CMS to be more clear about how it will protect Medicare claims data from revealing sensitive information about individuals or groups of patients.

CMS should ensure that any Medicare claims information released pursuant to a Freedom of Information Act request meets the HIPAA Privacy Rule standard for de-identification and has been de-identified pursuant to the Privacy Rule's statistician (or statistical) method. The statistical method requires that someone with "appropriate knowledge of and experience with generally accepted statistical principles" must determine that the "risk is very small that the information could be used, alone or in combination with other reasonably available information, by an intended recipient to identify an individual who is the subject of the information."[3] The statistical methodology, in contrast to the safe harbor, considers risk of re-identification based on whether the recipient of the data has the potential to reidentify, which yields a more particularized and accurate assessment of re-identification risk. Research has shown that the HIPAA statistical method of de-identification, if done appropriately, provides very strong protections for data while maximizing data utility.[4] In recent guidance on HIPAA de-identification, the HHS Office for Civil Rights also urges use of the statistical method.[5]

---

[2] *Sorrell et al. v. IMS Health Inc. et al.*, 131 S. Ct. 2653. 2011.
[3] 45 CFR 164.514(b).
[4] Khaled El Emam, Guide to the De-Identification of Personal Health Information (CRC Press, 2013).
[5] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html

However, de-identification – even using the statistical methodology – does not result in zero re-identification risk.[6] Consequently, we urge CMS to require recipients of Medicare claims data to execute written agreements prohibiting unauthorized re-identification.[7] Such agreements also can be vehicles for limiting the use of claims data to the agreed-upon purposes. Recipients of claims data found to have re-identified data without authorization, or to have used data in violation of the agreement, should be subject to administrative penalties, including, at minimum, being barred from future receipt of claims data.

CMS also should consider setting appropriate retention limits for data recipients (and requiring return or secure destruction of data at the end of the retention period), with the length of permitted retention dependent on the purpose for which the data is released. We also urge CMS to consider making claims data accessible without releasing the raw data, adopting an approach similar to that used by CMS in its Knowledge Discovery Initiative, currently being used to enable vendor access to data for internal CMS analytics purposes.[8]

As a final note, the risk to patient confidentiality does not just stem from unauthorized re-identification. Aggregate data about patients can be used to discriminate against, or otherwise harm, groups of patients. Breach of public trust in uses of Medicare data will jeopardize access to this data for important public purposes. It will be critical for CMS to carefully review requests for data and maintain sufficient oversight over proposed and actual data uses.

Conclusion

We are pleased to see that CMS has chosen to adopt a standard set of policies that will govern the disclosure of physician Medicare data. In light of the *Florida Medical Ass'n* court decision and CMS' commitment to transparency, we recommend the adoption of policies that will continue to evaluate FOIA requests for physician data based on whether the information will be used to further the public's interest as well as ensuring that patient privacy is protected through the use of statistical de-identification methods, appropriate data retention periods and carefully evaluating the use of aggregate data.

---

[6] McGraw, "Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data," J. Am. Med. Ass'n (2012), https://www.cdt.org/paper/building-public-trust-de-identified-health-data (open access).

[7] See Id.

[8] http://healthspottr.com/weeklydigest/34-5-reasons-to-like-the-cms-data-marketplace-initiative

We appreciate your consideration and thank you for the opportunity to provide comments and recommendations.

Sincerely,

Deven McGraw, Director, Health Privacy Project

Christopher Rasmussen, Policy Analyst, Health Privacy Project

On behalf of CDT and the following consumer organizations:
National Consumers League
National Partnership for Women and Families