Point32Health
1 Wellness Way
Canton, MA 02021
point32health.org

June 16, 2025

Robert F. Kennedy, Jr., Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Secretary Kennedy:

On May 16, the Department of Health and Human Services (HHS) released a Request for Information soliciting information regarding improving access to digital health products for Medicare beneficiaries as well as the state of the broader health technology infrastructure. We believe there is significant opportunity to advance technology as well as streamline and better align regulations in a manner that advances optimal patient experience while reducing healthcare costs.

Who We Are

Point32Health is a leading health and well-being organization, delivering an ever-better healthcare experience to everyone in our communities. Building on the quality, nonprofit heritage of our founding organizations, Tufts Health Plan and Harvard Pilgrim Health Care, we leverage our experience and expertise to help people find their version of healthier living through a broad range of health plans and tools that make navigating health and wellbeing easier.

Our programs take a 360-degree view of health for our members -- no matter their age, health, identity, or income. Our Foundation works with communities to support, advocate, and advance healthier lives for everyone and our Institute works to improve population health. We use empathy to understand what's important to those we serve, always making their priorities our own. We work to guide and empower people by bringing together wide-ranging partners and perspectives to create new approaches that make a real difference for both our industry and our 2.2 million members across the United States. We are proud that our Harvard Pilgrim Health Care Commercial Combined HMO, PPO and POS plans in Massachusetts and Maine, our Exchange HMO plans in Massachusetts and Maine, as well as Tufts Health Plan's Medicaid and Exchange HMO plans, have received full Health Equity Accreditation from the National Committee for Quality Assurance (NCQA). We are consistently a highly rated Medicare Advantage plan. For eight years, from Star Year 2016 to Star Year 2023, our Tufts Medicare Preferred HMO plan received a 5-star rating from the Centers for Medicare & Medicaid Services, the highest rating possible.

We are proud that Point32Health was recently recognized for the fourth time and the third year in a row as one of the 50 most community-minded companies in the nation by Points of Light, the world's largest nonprofit dedicated to volunteer service. A national standard for corporate citizenship, the Civic 50 showcases how leading companies are incorporating social impact, civic engagement, and community integration into their practices and values.

Overview of Our Comments

We appreciate that in the recent RFI, CMS has committed itself to policies that "reduce barriers to data access and exchange, realize the potential of recent innovations in healthcare that promote better health outcomes, and accelerate progress towards a patient centric health system." It was also helpful to see CMS specifically query if there is a role for CMS to advance adoption of digital health technology. We also recognize that throughout the RFI, there was a solicitation on ways to reduce provider burden.

In the attached appendix we provide detailed comments on how CMS can accomplish these goals. We recommend that CMS:

I. **Implement a Central Assessment Database for Digital Therapeutics (DTx) as well as a CMMI Model to Optimize Use:** Leveraging digital health products creates an opportunity to expand access to treatments for chronic disease, behavioral health and other areas. However, there are several obstacles to this pathway. First and foremost: Payers, clinicians and patients must be confident in the efficacy of a digital health product. The sheer number of products makes this impossible for a typical clinician and patient as well as extremely costly for regional health plans. While some digital products have been developed using rigorous methods and evaluated through randomized clinical trials, others lack foundational rigor. Sifting through an ocean of potential products to find the clinical "pearls" is a laborious process. We recommend the federal government establish an easily searchable database that includes critical elements regarding digital therapeutics (DTx), including the results – or absence – of clinical trials. The database would identify certain products with an "E-Healthy" icon (e.g. ones that meet certain clinical evidence and other standards). We also recommend that CMMI launch a model where Medicaid and Medicare Advantage plans are incentivized to integrate the use of certain "e-healthy" digital therapeutic products into primary care provider (PCP) practices and emergency room discharges. For instance, while stabilizing patients, many emergency rooms realize the patients also have behavioral health issues (e.g. alcoholism). Through this CMMI program, ERs could enroll exiting patients in appropriate DTx therapies, instead of leaving with only a list of recommended clinics where appointments are likely to be difficult to obtain. Similarly, PCPs could be supported to enable them to enroll patients struggling to manage their chronic disease into DTx dedicated to diabetes, asthma or other chronic disease patients.

II. **Reduce Provider Burden and Administrative Costs through Enhanced Electronic Medical Record (EMR) Accessibility:** Despite the fact that the vast majority of Medicare providers have invested in electronic health records, provider administrative burden remains significant and problematic. The positive potential of EHR adoption has been undermined because remote access to EHRs usually isn't granted to payors at all, or only at an additional cost. In some cases, this is because the EHR vendors require providers to purchase additional licenses if payors are allowed to remotely access the EHR. As a result, providers must continue to use faxes and other outdated modes to communicate to health plans. This is unfortunate, as most of the abrasion providers experience in the prior authorization process – the back and forth via phone and fax regarding payor requests for additional information – could *immediately* be avoided if payors were simply given remote access to the EMR. *This is possible today, with virtually no additional technology enhancements by providers or payors.* We recommend the federal government update its

current Certified Electronic Health Record (EHR) Technology (CEHRT) to require EHR vendors to allow providers to grant remote access to payors without an additional fee, and for providers to do so, for treatment, payment and health care operations as defined by HIPAA.

III. **Streamline Regulatory Deadweight to Unburden Payor Technology Budgets:** Insurers are regulated by numerous Agencies of the Federal Government – and even within HHS, individual departments have differing priorities. Ultimately, most of these regulations drain the budgets of payor technology departments. This means that payors must allocate scarce technology resources to initiatives that their members neither want nor ultimately use. For instance, individual health plans spent millions of dollars implementing the Medicare Prescription Payment Plan (MPPP). At this time, member participation is less than 1%, according to estimates by Milliman. This is especially problematic for regional not for profit health plans. According to MedPAC, "plan-reported margins vary by a plan's tax status and whether a plan is a SNP. In the 2022 data, nonprofit plans reported a margin of 0.1 percent…." To liberate technology resources for member demanded services that actually improve healthcare, we urge the Administration to
    a. *Use Technology to Improve RADV and the Medicare Risk Adjustment Program*
    b. *Synthesize Transparency Rules*
    c. *Proactively Defend Private Sector Entities and Streamline Cybersecurity Regulations*

The healthcare environment presents increasingly complex challenges as we strive to maintain affordability, improve health outcomes, and comply with evolving regulatory expectations. We appreciate this important initiative by the federal government. We believe the recommended adjustments outlined below will support the dual goals of improving quality of care while advancing operational sustainability and rationalizing healthcare expenditures.

Thank you for considering our perspectives on these important issues. We look forward to continued collaboration to advance a stable, affordable, and accessible healthcare system. Please contact Christina.Nyquist@Point32Health.org if we can provide additional assistance.

Sincerely,

Christina Nyquist

Christina Nyquist

Vice President, Federal Affairs

Appendix

I. **Implement a Central Assessment Database for Digital Therapeutics (DTX) as well as a CMMI Model to Optimize Use (PC-5, PC-6, PC-7, VB-1):** Leveraging digital health products creates an opportunity to expand access to treatments for chronic disease, behavioral health and other areas. However, there are several obstacles to this pathway. First and foremost, payers, clinicians and patients must be confident in the efficacy of a digital health product. The sheer number of products makes this impossible for a typical clinician and patient as well as extremely costly for regional health plans. While some digital products have been developed using rigorous methods and evaluated through randomized clinical trials, others lack foundational rigor. Sifting through an ocean of potential products to find the clinical "pearls" is a laborious process.

Recommendations: We recommend the federal government:

a) **Create a Digital Therapeutics Transparency Advisory Board (D-TAB):** We believe a foundational action would be for the federal government to establish a Digital Therapeutics Transparency Advisory Board (D-TAB). This advisory board would include representatives from clinicians (including hospitals, family physicians, and psychologists), public payors (including Veterans Affairs, Health and Human Services and state Medicaid programs), the digital therapeutics industry, patient groups (including senior citizens and veterans), underserved communities (including representatives of racial minorities and rural areas), and private payors (including regional and not for profit health plans).

A necessary step towards transparency would be recognizing the different levels of digital categories nested within each other. The largest of the categories is digital health which includes a variety of wellness trackers, telehealth platforms, diagnostics, and other digital tools. Within this large category lies a smaller subset known as Digital Therapeutics (DTx). These products are specifically designed to treat, manage, or prevent a disease with software as the primary intervention method. They may be used independently or in conjunction with drugs, devices, or other therapies to optimize patient outcomes. DTx products should comply with best practices to ensure product integrity, incorporate user-centered design, protect patient privacy, and have validated clinical outcomes via randomized controlled trials and real-world evidence. It is critical for D-TAB to use a definition of digital therapeutic (DTx) which appropriately applies a higher level of rigor and clinical evidence than for products in the larger digital health space.

The Digital Therapeutics Transparency Advisory Board (D-TAB). should have three primary roles: the establishment of a transparent database of clinically effective digital therapeutics; advising CMMI on the development of a digital CMMI model; and publishing an annual report on real-world evidence on digital health.

b) **Transparent Database**: First, D-TAB should design and develop a transparent, easily searchable inventory of digital therapeutics that include the following searchable categories:

i. Conditions (e.g. depression, schizophrenia, anxiety, bipolar disorder, dementia, substance use disorder, etc.) the therapeutic is designed to manage.

ii. Size of Randomized Controlled Trial (if D-TAB chooses to expand database beyond products with RCTs, then D-TAB should specify the minimum requirements of such alternative evidence for safety and efficacy).

iii. Outcome of Randomized Controlled Trial (using D-TAB developed metrics described below).

iv. Cultural Considerations and Language Options (e.g. Portuguese, Cantonese, Mandarin, etc.).

v. Broadband required/not required.

vi. Equipment needs (phone, tablet, laptop, VR, wearable, etc.).

vii. Cybersecurity certifications.

viii. Findings from other independent evaluations (e.g. FDA, etc.).

ix. Compliance with HIPAA and other privacy standards.

x. Ability to collect health equity metrics.

xi. Savings estimates (e.g. clinical costs, administrative savings)

xii. Expanded access opportunities.

xiii. "E-Healthy" Recommendations: Products that meet the D-TAB recommendations regarding clinical evidence, cybersecurity and privacy compliance should be labeled with an "E-Healthy" icon."

xiv. Precautions: this section would provide warnings regarding contraindications for specific digital therapeutics, information on recognized adverse events, etc.

xv. Target Populations: this section would provide information regarding which populations are most suited for the product.

This database tool should be designed with a user experience that includes simple, high-level information written in a patient friendly format. However, it also should include functionality that enables medical professionals to obtain more technical findings in an equally accessible manner.

D-TAB should establish a process that would assure the timely, ongoing updating of the database. New therapeutics are emerging at a rapid pace, so the database should be updated at

least quarterly. *Initially limiting the database to therapeutics with a very high standard of evidence – such as Randomized Controlled Trials – will also make launching and maintaining the database more manageable*

b) **Digital CMMI Model**: Second, the advisory board should advise the Centers for Medicare and Medicaid Innovation (CMMI) on the establishment of a model where participating Medicaid and Medicare Advantage plans would be reimbursed for integrating the use of "e-healthy" designated digital therapeutic products into:

   i. *Primary Care*: Health plans participating in the CMMI model would establish a mechanism to educate PCP practices regarding "E-Healthy" digital therapeutic options that meet specific efficacy standards, reimburse PCP staff for helping patients initially enroll in effective digital therapeutics, and use "best practices" to incorporate data from the digital product into ongoing treatment.

   ii. *Emergency Room Discharge Process*: Health plans participating in the CMMI model would educate emergency room staff regarding highly effective "E-Healthy" digital therapeutics and implement reimbursement for staff to enroll appropriate patients upon discharge.

   iii. *Other clinical care locations*: In addition to primary care and ER discharge, D-TAB should consider whether other clinical care settings should be incorporated as well. For instance, perhaps endocrinologists should be incorporated to expand enrollment of patients with diabetes or specialists responsible for patients with other chronic medical conditions. D-TAB also should evaluate if certain licensed clinicians – other than-physicians -- should be allowed to prescribe "E-Healthy" digital therapeutics (e.g. psychologists, licensed social workers, etc.)

c) **Real-World Evidence on Digital Health Report**: D-TAB should recommend specific real-world data metrics that participating CMMI payors would collect regarding digital product usage by patients and the associated health outcomes. This real-world evidence would be published and utilized to further refine the digital model and best practice recommendations. Health equity metrics would be part of this report.

d) **Other Responsibilities**: In their advisory capacity for a digital CMMI model, D-TAB should also make recommendations regarding:

   i. *Conditions and Efficacy Metrics*: D-TAB would specify the conditions where digital therapeutics should be leveraged. We recommend the advisory panel NOT limit the conditions to behavioral health only. As described above, there is a strong interplay between physical health and behavioral health. Therefore, we recommend that digital therapeutics effective at treating physical conditions such as diabetes should be included. D-TAB should recommend evaluation criteria for digital therapeutics designed for different condition categories. For instance, the appropriate metric for a diabetes product might be improvement in A1c levels. DTx products that meet D-

TAB's recommendations regarding clinical efficacy, cybersecurity and other standards should be clearly demarcated in the database as "E-Healthy" products. These "E-Healthy" products would be the only ones covered in the CMMI digital model and where participating payors and providers would be reimbursed for "prescribing" to patients.

ii. *Underserved Populations*: The advisory board should make recommendations on the best way to assure low-income individuals are able to access "E-Healthy" therapeutics. For instance, CMMI may reimburse payors for having case managers assist members in applying to governmental programs that subsidize cell phone costs, broadband or perhaps to directly provide "health only" tablets whose only available apps are health-related ones prescribed by their clinician team.

iii. *Best Practices*: D-TAB should recommend best practices for onboarding of patients with digital products, clinician use of digital data (recognizing the limited time availability of primary care and other clinical practices), and other areas to optimize patient outcomes in the most efficient manner.

iv. *Codes*: D-TAB should coordinate with other coding stakeholders to make recommendations to assure that the full spectrum of care associated with the use of digital therapeutics have appropriate codes available

II. **Reduce Provider Burden and Administrative Costs through Enhanced Electronic Health Record (EHR) Accessibility (PC-8 PR-2, PR-3, PR-7, PR-12, PR-13, PA-5, TD-9, TD-11):** In 2020, the federal government established that if providers fail to adopt certified electronic health record (EHR) technology (CEHRT), Medicare can reduce their payment levels. Despite the fact that over 88% of Medicare providers have invested in electronic health records, provider administrative burden remains significant and problematic. The positive potential of EHR adoption has been undermined because remote access to EHRs usually isn't granted to payors at all, or only at an additional cost. In some cases, this is because the EHR vendors require providers to purchase additional licenses if payors are allowed to remotely access the EHR. As a result, providers must continue to use faxes and other outdated modes to communicate to health plans. This is unfortunate, as most of the abrasion providers experience in the prior authorization process – the back and forth via phone and fax regarding payor requests for additional information – could *immediately* be avoided if payors were simply given remote access to the EMR. *This is possible today, with virtually no additional technology enhancements by providers or payors. Providers and EHR vendors just need to make the EHR remote access available without additional licensing fees.* The Health Insurance Portability and Accountability Act (HIPAA) Privacy rules already apply to payers, and patient data would remain secure.

Recommendation: This could be accomplished very quickly if CMS were to update the CEHRT standards. We recommend that in order to be considered as using certified health record technology:

a) the EHR vendors must allow payor organizations to remotely access a provider's EHR *for treatment, payment and healthcare operations* as defined by HIPAA, without the imposition of additional fees onto the provider client or the payor entity.

b) the provider licensing the EHR must allow payor organizations to access a provider's EHR *for treatment, payment and healthcare operations* as defined by HIPAA, without the imposition of additional fees onto the payor entity.

This will decrease administrative costs as it will reduce provider burden in numerous interactions with health plans. With regard to prior authorization, doctor offices would no longer receive routine faxes or phone calls requesting additional patient data after an initial prior authorization is submitted. Instead, the insurer's case management nurses would remotely access the patient's record to locate the data in question and then approve the prior authorization. Additional data access significantly expedites the approval of a prior authorization submission. Mandatory remote access to EHRs would decrease provider burden in other areas as well. For instance, as part of the risk adjustment process (in both commercial ACA and Medicare Advantage), payers require additional "chart" information from providers. Remote EHR access would reduce current provider burden involved in manually copying and sending such information. Similarly, doctors must provide quality information data to health plans for STAR ratings in Medicare Advantage. Remote EHR access would improve this situation as well.

III. **Streamline Regulatory Deadweight to Unburden Payor Technology Budgets (TD-19, PR-7, TD-17)**: Insurers are regulated by numerous Agencies of the Federal Government – and even within HHS, individual departments have differing priorities. Ultimately, most of these regulations drain payor technology budgets. This means that payors must allocate scarce technology resources to initiatives that their members neither want nor ultimately use. For instance, individual health plans spent millions of dollars implementing the Medicare Prescription Payment Plan (MPPP). At this time, member participation is less than 1%. This is especially problematic for regional not for profit health plans. According to MedPAC, "plan-reported margins vary by a plan's tax status and whether a plan is a SNP. In the 2022 data, nonprofit plans reported a margin of 0.1 percent…." These narrow margins provider little room for unnecessary or suboptimal technology expenditures. To liberate technology resources for member demanded services that actually improve healthcare, we urge the Administration to

a) **Synthesize and Consolidate Transparency Requirements (TD-19)**: We support transparency and the ability of patients to make informed choices when selecting providers and procedures. However, currently, health plans are impacted by numerous existing or imminent transparency-related regulations including: the RXDC report, the Transparency in Coverage Cost Estimator, Machine-Readable Files for Medical Information, Machine Readable Files for Drugs, Interoperability 1.0 and 2.0, and the Advanced Explanation of Benefits (AEOB). Implementation of and ongoing compliance with these regulations are costly and some of these overlapping provisions are not necessary to achieve transparency. The significant expenditures in these areas is frustrating, given there has been little uptake in many of these areas, including the use of machine-readable files on which *each* health plans spent millions of dollars implementing.

We urge the federal government to conduct a holistic review of all transparency related regulations and synthesize a single cohesive and cost-effective framework that provides transparency to members. *Part of this should be requiring the correct entity to provide transparency.* For instance, with regard to any drug information – transparency requirements should be imposed on the PBM or the pharmaceutical manufacturer – not the health plan. Health plans lack complete access to drug pricing and other related information as much of this is considered proprietary by PBMs and housed in their systems only.

Another example is the AEOB rule. The AEOB regulation has not yet been promulgated. Instead of creating a completely new process for health plans to implement, we urge the Administration to consider the transparency tools *that already have been developed.* There are two previously launched initiatives that could be leveraged to execute the new AEOB requirements.

- First, every health plan already publishes extensive machine-readable files on the negotiated costs for medical services with their health plan. These files have largely been unused by the public.
- Second, the federal government has launched the National Plan and Provider Enumeration System (NPPES), which is publicly accessible. It is a system administered by the Centers for Medicare & Medicaid Services (CMS) to assign unique identifiers, called National Provider Identifiers (NPIs), to healthcare providers.

The federal government could explore combining these two initiatives to execute the AEOB. The NPPES portal could be expanded to allow providers to initiate a patient request for an AEOB. This government system could then access the machine-readable files already published to the cloud to generate a personalized AEOB for the patient. This would be an efficient implementation of AEOB because, rather than each individual health plan designing and funding individual portals (and providers being frustrated from multiple access points), the federal government would create a single AEOB point and leverage existing machine-readable file infrastructure. This government-led combination would be more uniform, less expensive, and would increase compliance while furthering the administration's goal of transparency. In addition, this would help reduce the likelihood that regulation writers would significantly underestimate the cost of their regulations because the federal government would be responsible and could not simply shift these tremendous costs onto the private sector.

b) **Proactively Defend Private Sector Entities from Cyber Warfare and Streamline Cybersecurity Regulations:** An expensive, recurring, and increasing issue in the healthcare industry is ransomware attacks. Highly sophisticated and organized entities, sometimes funded by foreign governments, attack hospitals, health plans, and other healthcare stakeholders and threaten to expose patient information if a ransom is not paid. In a recent year, there were 181 confirmed ransomware attacks on healthcare providers with an average ransom payment of $900,000 per attack, resulting in a total of $162.9 million paid in ransoms. In 2024, Change Healthcare paid a $22 million ransom to prevent the release of

stolen data, only for the attacker to provide the stolen data to another group who then attempted to extract a further ransom payment. In addition to ransom payments, there are many other costs related to healthcare cyberattacks: recovery efforts, legal fees, communications, etc. Change Healthcare's parent company, UnitedHealth Group, confirmed that losses in 2024 due to the attack had risen to $2.9 billion. In 2023, the cost of all combined healthcare data breaches due to cyberattacks was estimated at $7.93 billion.

At the same time, we are concerned that federal agencies have begun to issue rules that differ from other agencies as well as industry gold standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Currently, health plans must abide by standards and regulations which conflict and overlap, such as Sarbanes-Oxley, HIPAA, etc. Additionally, most states have their own unique cybersecurity regulations that can conflict with or duplicate federal regulations, creating even more administrative burden for health plans. It is important to focus stakeholder financial resources on optimizing their technological defense, not on unnecessary administrative burdens. Streamlining and consolidating federal cybersecurity requirements into a single comprehensive framework can reduce administrative costs, improve efficiency, and enhance incident response. The two most recent examples of problematic regulatory over-reach include:

i. **Cyber Incident Reporting for Critical Infrastructure Act**: The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule's requirements for reporting cyber incidents would force health plans to report any cyber incident multiple times, when they are already required by other agencies to do so. All health plans are required by HIPAA to report these incidents; they are then bound by CIRCIA to go through the same process with a different agency, all while dealing with a cybersecurity incident. This duplicative and unnecessary reporting requirement diverts important resources away from critical incident response activities and forces health plans to put those resources into administrative reporting.

ii. **Office of Civil Rights (OCR) HIPAA Security Rule Modifications NPRM**: While we support the necessity of adaptation and dynamism in cybersecurity regulation, we are concerned that the proposed revision of the HIPAA Security Rule would impede an organization's ability to bolster substantive cybersecurity technologies as it would divert significant resources to unnecessary, confusing, and counterproductive administrative requirements.

Recommendations: Instead of the CIRCIA rule's approach, we urge the federal government to designate a single "gold standard" for cybersecurity – such as NIST CSF 2.0. Each agency could require adoption or certification of compliance with the gold standard, rather than promulgate its own regulations. Organizations who obtain independent certification with these federal gold standards should be provided with a safe harbor to be protected from class action lawsuits. Finally, there should be federal incentives for state standards to be aligned with this gold standard. The federal government should also create and manage a central reporting framework that allows entities bound by reporting regulations to other federal agencies to only report once, to

which the information can then be shared between agencies. Finally, we urge that the OCR HIPAA Security Rule notice of proposed rulemaking be withdrawn.

Furthermore, we urge the Administration to aggressively investigate, identify, and hold accountable the criminal entities that are carrying out these crimes against private businesses. These efforts should include investigating past cyberattacks on private businesses aimed at recovering ransoms that have been paid by the victims of these crimes. We also recommend the Administration take immediate steps to reduce the potential profitability and, therefore, the incentive to commit these crimes. For example, the Administration could implement regulations that would enhance the traceability of Bitcoin and other cryptocurrency transactions, and it could increase efforts to police the "Dark Web" to identify individuals or entities that illegally publish individually identifiable personal information. Private companies that are the victims of these crimes suffer significant financial harm, which can result in closures and loss of jobs. Often the victims are subject to extensive audits from federal and state agencies while they are attempting to recover from these sophisticated cyberattacks. Rather than spending significant resources re-victimizing the victims, the federal government should be proactively working with private entities, including healthcare providers and insurers, to share information and best practices to increase the country's overall cybersecurity posture.

c) **Use Technology to Improve RADV and the Medicare Risk Adjustment Program (PR-7, TD-17):** We appreciate the Administration's commitment to program integrity. We understand the interest in Risk Adjustment Data Validation (RADV) audits. Medicare Advantage plans must be good financial stewards in providing critical Medicare benefits. However, the current RADV audit system is unnecessarily administratively burdensome and inefficient at policing plan practices. As such, the current program is unnecessarily costly to the federal government while its administrative costs disproportionately hurt not for profit health plans who are less able to amortize the significant expenditures. The following suggestions would improve the effectiveness and efficiency of RADV audits and the risk adjustment program overall.

   i. **Automate Prevention of Questionable Coding Practices:** The federal government currently focuses only on "retroactively" trying to "catch" problems. Many of these could be proactively prevented in the first place. The federal government could calibrate Encounter Data Processing System (EDPS) filtering logic so that it would "reject" plan submission of records or codes that CMS identifies as likely to be erroneous. For example, when a physician office visit includes an acute stroke code – without a corresponding recent emergency or hospital inpatient claim – this is likely a miscode documenting a history of stroke, rather than treatment of stroke. This is a critical differential in risk adjustment payment. A filter could block submission of codes in this scenario. This increases efficiency as it proactively prevents overpayments on the front end -- rather than the government trying to claw back costs through RADV audits. In addition, this is likely to save more dollars

that retroactive audits, as a filter would catch every one of these situations, whereas an audit might not have a result as comprehensive.

ii. **Streamline Data Collection for Quality Control**: Despite the widespread adoption of electronic medical records, many health plans who seek to exert quality control over their risk adjustment practices are forced to conduct laborious manual reviews. To aid health plans that seek to improve the accuracy of their risk adjustment, providers should be required to make EMR data available for treatment, payment and health care operations. EMR vendors and Health Information Handlers (HIH) that contract with provider organizations to manager their medical charts should be required to allow this remote access or provide the charts directly to the health plan directly in a timely manner and without the imposition of additional costs. These requirements should be part of an updated set of CERHT rules.

iii. **Mitigate Gaming by Prohibiting Specific Practices:** A more efficient approach then massive RADV audits, would be to first prohibit specific practices that are likely to enable gaming. Specifically, the federal government should:

1. ***Prohibit plans that have a stake in a risk adjustment vendor*** (i.e. subsidiary that provides chart review services or in-home HRAs) from using those companies in their own risk adjustment processes

2. ***Require that charts be reviewed*** for codes that should be *deleted* as well as added. This is similar to requirements under the ACA Risk Adjustment program and Edge Submission protocols.

3. ***For health plans that own provider entities***, exclude profits from related provider entities that revert to the parent or another parental subsidiary from the health plan's medical expenses when the related insured entity submits its MLRs to CMS

4. ***Restrict Physician Incentives for Upcoding*:** For all health plans, restrict providing payment contingent on providers certifying and reporting *all* the codes proposed by health plan vendors.

5. ***Codify In-Home Assessment Best Practices:*** *When a health plan sponsors an in-home assessment, information collected must be provided to a primary care provider. Information should trigger a patient care plan, if appropriate. Diagnoses that are found only via an in-home assessment should be subject to a secondary quality assurance review by a certified medical coder.*

iv. **Disseminate Best Practices for "Sentinel" Impact:** The federal government should clearly outline their position on best coding practices. Unfortunately, current coding guidelines are vague in many areas and leave things to "judgement" of coders. As a result, conservative health plans will voluntarily moderate those coding practices.

However, aggressive plans can defend their practices as within "judgement." Historically, the federal government has been leery to reveal audit criteria. However, if the federal government did lay out more detail, they would impact a much larger portion of the market. Instead of only catching the claims that happen to be part of the audit – they would proactively influence a wide swath of the marketplace. Even a "large" audit will be a relatively small portion of actual claims processed.

v. **Target RADV Audits to Optimize Recoupments:** RADV audits require a significant investment on the part of the federal government and are costly endeavors. Rather than do this for every plan every year, CMS should target audits to plans that are most likely to generate significant recoupments from the audit. These targets could be identified by certain characteristics. For instance, MA plans that conduct chart reviews should not just be submitting code additions that they find in charts. They also should be submitting code *deletions* because chart reviews also should identify codes that were in error. Any health plan whose addition submissions are disproportionate to its deletions, should be identified for an audit. In addition, audits could be targeted against with significant risk adjustment deviations from industry average. For example, plans which *have all three of the following characteristics:* a minimum number of lives or member months greater than or equal to the specified level of credibility above a 1.0 normalized risk scorerisk score growth above industry average, over a multi-year period

vi. **Provide Sufficient Time for Audits:** The recently-announced timeframe for the Medicare Advantage RADV audits will be very problematic for health plans – especially smaller plans that rely on relationships with independent providers. Responsible health plans spend considerable time curing their risk adjustment data for quality control. Because Medicare has been historically behind in its RADV audits, many plans have not yet completed these reviews for more recent years (e.g. 2022, 2023). We urge the Administration to allow plans additional time to cure data for those years. In addition, we also encourage the Administration to recognize that provider cooperation is critical for MA plans to complete quality control. Therefore, we ask CMS to require providers make data available to health plans on a timely basis. If they have electronic medical records, they should make that available remotely to health plans (see above recommendation). If they lack EMRS, then they should provide medical records within one week of the plan request at no additional cost to the health plan. Moreover, if a health plan requests data but the provider fails to provide on a timely basis, health plans should not "fail" samples for which plans demonstrate best faith efforts to obtain records for but are not successful in obtaining from providers.

vii. **Include a Fee For Service Adjustor:** When the federal government does conduct RADV audits, we are concerned about the financial impact of extrapolating the results. If the federal government does intend to use extrapolation, it is critical that it utilize a "fee for service" adjustment against the error rate. It would be

inappropriate to hold the Medicare Advantage system to a higher standard than the fee for service Medicare program. MA plans should only be held to the portion of an error rate that exceeds the error rate of the traditional fee for service program.