December 26, 2019

Ms. Joanne Chiedi
Acting Inspector General
Office of Inspector General
Department of Health and Human Services
Washington, DC 20201

Dear Ms. Chiedi:

On behalf of the Healthcare Information and Management Systems Society (HIMSS) and the Personal Connected Health Alliance (PCHAlliance), we are pleased to provide written comments to the Notice of Proposed Rule Making (NPRM) on *Medicare and State Healthcare Programs: Fraud and Abuse; Revisions To Safe Harbors Under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements (File Code: OIG-0936-AA10-P).* HIMSS and PCHAlliance appreciate the opportunity to leverage our expertise in offering feedback on safe harbor protections under the federal Anti-Kickback Statute for certain coordinated care and associated value-based arrangements as well as new safe harbors for donations of cybersecurity technology and amending the existing safe harbors for electronic health records (EHRs) arrangements. We look forward to continued dialogue with the Office of Inspector General (OIG) on these and other public policy topics relevant to health information and technology.

HIMSS is a global advisor and thought leader supporting the transformation of the health ecosystem through information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and analytics to advise global leaders, stakeholders and influencers on best practices in health information and technology. Through our innovation engine, HIMSS delivers key insights, education and engaging events to healthcare providers, governments and market suppliers, ensuring they have the right information at the point of decision. Headquartered in Chicago, Illinois, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East and Asia Pacific. Our members include more than 80,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations.

PCHAlliance, a membership-based HIMSS Innovation Company, accelerates technical, business and social strategies necessary to advance personal connected health and is committed to improving health behaviors and chronic disease management via connected health technologies. PCHAlliance is working to advance patient/consumer-centered health, wellness and disease prevention. The Alliance mobilizes a coalition of stakeholders to realize the full potential of personal connected health. PCHAlliance members are a vibrant ecosystem of technology and life sciences industry icons and innovative, early stage companies along with governments, academic institutions, and associations from around the world.

HIMSS and PCHAlliance are supportive of the transformation underway of our healthcare system, and the push for better value and outcomes as a top priority of the Department of Health and Human Services (HHS). We encourage HHS to review established practices and enhanced collaboration opportunities among providers and other individuals and entities as a potential way to reinforce this transformation. The modification of existing safe harbors and addition of new protections will help remove barriers to more effective coordination and management of patient care and delivery of value-based care. Overall, updates to the Anti-Kickback Statute are critical to improving quality of care, health outcomes, and efficiency.

As described in this Proposed Regulation, OIG's Anti-Kickback Statute proposal includes almost identical changes to the Centers for Medicare & Medicaid Services (CMS) Physician Self-Referral Law proposal. HIMSS and PCHAlliance aligned our comments for both proposals to ensure consistency and to amplify our messages.

With these factors in mind, HIMSS and PCHAlliance offer the following thoughts on the policies included in the proposed regulation:

Ensure Greater Clarity Around Technologies and Entities that Can Engage the Safe Harbors as a Value-Based Enterprise (VBE) Participant

HIMSS and PCHAlliance support and advocate for policy and practices that lead to adoption of evidence-based care management, including remote patient monitoring and digital tools that support delivery of quality health care. Value-based arrangements, when structured to include the evidence-based tools providers need to deliver care, enable effective and efficient care delivery that improves care quality while reducing health costs.

We share the HHS goal for two-sided risk, value-based arrangements to thrive in health care reimbursement models in the near-term. However, to achieve that goal, it will be necessary for all health technology evidence-based tools to be included as risk-based participants in value-based arrangements. Specifically, providers, who deliver and manage care for their patients, must be able to negotiate and obtain contracts for the tools and services they need and use in a manner that incentivizes those tools and services to improve care through better outcomes and lower costs.

HIMSS and PCHAlliance support the application of Anti-Kickback Safe Harbor protections for the potential VBE participants specified in the Proposed Regulation. In addition, we endorse the inclusion of additional VBE participants, including: health technology companies; medical device manufacturers; and, manufacturers, distributors, or suppliers of durable medical equipment, prosthetics, orthotics or supplies (DMEPOS). Each of these entities is integral to creating value for patients and payors by improving the coordination and management of patient care, reducing inefficiencies, or lowering health care costs.

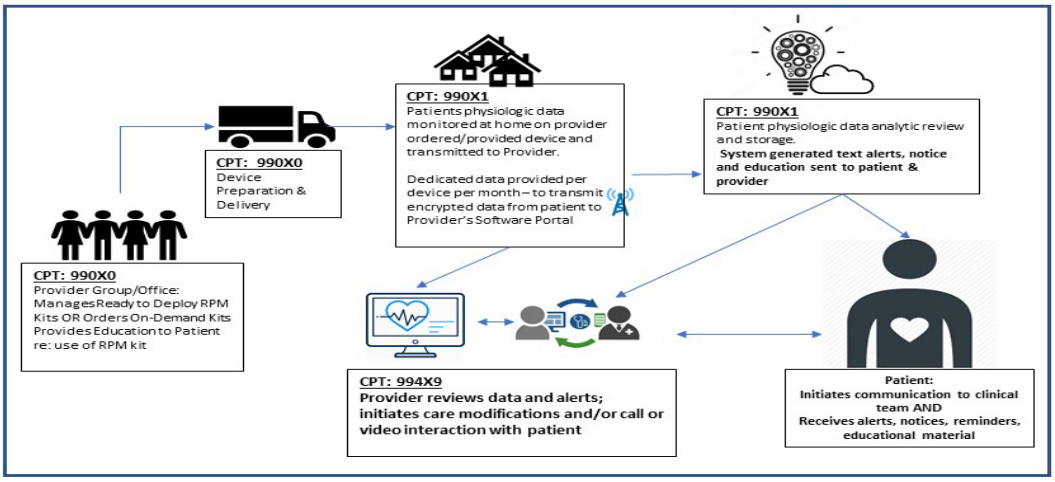
HIMSS and PCHAlliance would like to be a resource and continue to provide assistance and guidance that will lead to improved adoption of risk-based reimbursement. Included below are additional comments to support the inclusion of these additional VBE participants in safe harbor protections. We hope this information provides OIG with

greater clarity—based on our reading of the Proposed Regulation, we are unclear what the agency is seeking to prevent in terms of the inclusion (or exclusion) of additional entities as VBE participants.

- *The Proposed Regulation as structured will exclude health technology companies and health applications, such as remote patient monitoring*

The Food and Drug Administration (FDA) regulates medical and clinical software as a medical device. Specifically, remote patient monitoring is noted in the Proposed Regulation as a desired function for care coordination and management. Therefore, it is desirable as part of a VBE, and is defined and regulated as a medical device. Remote patient monitoring, ordered by a provider, includes both standalone software (defined as a medical device) and a medical device (ordered by the clinician to provide the bio-physical data needed for care management, e.g. blood pressure, oxygen levels, weight). This information is collected and transmitted to the clinician as specified patient-generated health data via software linked to both the patient and the provider (see figure A).

Figure A



The exclusion of medical device entities from VBE will exclude technology platforms, including remote patient monitoring or other technology innovations that lead to improved outcomes and costs of care. Software and remote communication capabilities are integral, and expected, components of today's medical devices.

For example, as described in this proposed regulation, health technology companies and medical device manufacturers play an important role in care coordination and provide the types of digital and mobile health technology (like remote monitoring, data analytics, patient portals, and other communications) that OIG states "hold promise for improving care coordination and health outcomes through monitoring of real-time patient data and detection and prevention of health problems" (Page 55705).

In addition, one of our member organizations described how they are working on a joint venture with a physician-led health system in which they are analyzing the health

system's population health data in order to identify clinical drivers of hospitalization risk and interventions available to mitigate risk for various types of heart failure patients. This partnership aims to deploy new tools that help clinicians intervene earlier and better manage patients with heart failure, with the ultimate goal of reducing avoidable emergency department visits or hospitalizations. Expanding the Safe harbor will allow companies participating in these types of arrangements to pursue relationships with other entities and realize the objective of maximizing their shared savings potential.

As a result, the broad exclusion of medical device manufacturers may stifle areas of innovation and lead to incongruous corporate structuring that separates health technology from a medical device, which may not be in the patient's best interest.

Finally, we acknowledge the importance of pharmaceutical manufacturers in the delivery of value-based care, but we recommend that OIG evaluate and assess the complexities that would be involved with including these manufacturers as a VBE participant.

- *Given that federal medical and health device definitions already exist, do not prioritize the development of another definition that will confuse regulatory and reimbursement systems rather than improve patient care*

OIG seeks input on the definition of a medical device, but between FDA as well as CMS, definitions being used in the federal government already exist. Another definition is likely to create extensive burden for companies and present an opportunity for fraud by nefarious scammers. Under FDA guidance, software is a device, while Medicare distinguishes between medical equipment distributed by physicians (such as an ambulatory blood pressure monitor or glucose meters) versus that distributed by suppliers (continuous glucose monitors, walkers, knee braces, etc.). We encourage OIG to employ the FDA and CMS definitions of a medical device rather than promulgate its own version.

- *A full range of evidence-based tools and services will be needed to make value-based enterprises successful*

Full risk sharing that incentivizes patient-centered, outcomes-driven care delivery can only flourish if all providers are able to access and use evidence-based tools and practices. Technology is a crucial part of the health care provider's toolbox and the proposal to exclude "medical equipment" will exclude clinical software, which is regulated and defined by FDA as a medical device. For example, remote patient monitoring for chronic disease is associated with reduced complications, reduced hospitalization rates, and better outcomes. This technology includes connected medical devices that deliver patient-generated data to clinicians through clinical dashboards (software), chosen by a clinician. If medical devices (which by regulation includes software and the clinical dashboards that providers lease or purchase) are excluded from VBE, adoption of value-based arrangements will be significantly slowed because:

  - Providers will be unable to share a portion of the risk associated with patient outcomes with their care management services vendors. They will delay entering into such arrangements until they have developed more extensive fee- for-service-based experience with remote monitoring and digital tools

- Small and mid-size providers, unable to share risk with the tools and services they contract for, are unlikely to be able to shoulder full risk
- Health technology may be less incentivized to deliver and innovate for improved outcomes and efficiency, leading to product development that does not drive toward value-based care

Continuous clinical support offered through value-based arrangements that include medical device manufacturers as a participant would help ensure that a patient's needs are met throughout the entire course of treatment. OIG's exclusion of health technology companies; medical device manufacturers; and, manufacturers, distributors, or suppliers of DMEPOS means that payment exchanged as part of a value-based arrangement involving one of these entities would not receive protection from Anti-Kickback Statute liability under OIG's proposed new safe harbors for value-based arrangements or new safe harbor for patient engagement support and tools.

OIG asserts that these entities would not be permitted to make outcomes-based payments protected under the agency's proposed revisions to the personal services safe harbor. For example, if there is an arrangement that involves outcome-based payments for devices, services, or care management based on a reduction in costs to the healthcare system, it could serve as an appropriate incentive for providers not to simply provide a product to a chronic disease patient, but to encourage better outcomes at lower costs.

Under the proposed example, this arrangement would not be allowed. This absence would have a dramatic impact on health technology companies; medical device manufacturers; and, manufacturers, distributors, or suppliers of DMEPOS as millions of patients could lose access to innovative care and technology development that is halted due to uncertainty around the application of these safe harbors.

Overall, we urge OIG to allow providers to share risk for outcomes with the developers and suppliers of the tools they believe will improve care and reduce costs.

Institute a Waiver or Reduction of Cost-Sharing Obligations for Care Management

HIMSS and PCHAlliance urge the creation of a safe harbor that permits providers to waive cost-sharing for care management, defined as the CPT codes listed in the CY2020 Medicare Physician Fee Schedule Table of Care Management Codes, when the cost-sharing for the month's care management services does not cover the administrative costs associated with billing. For the purposes and ease of administration, we recommend the safe harbor be provided for care management services, as these are non-face to face services associated with care coordination and management when the cost sharing is $10 or less. Such arrangements will promote patient engagement and support improved quality, health outcomes, as well as efficiency.

Create a New Safe Harbor for Donations of Cybersecurity Technology

Currently, no safe harbor exists for this particular area, but HIMSS, PCHAlliance, and the broader stakeholder community have all identified it as a genuine need. Under its authority, OIG is proposing an exception to protect arrangements involving the donation

of certain cybersecurity technology and related services. We overwhelmingly support OIG for taking this major step forward, as it represents a fundamental acknowledgement that this safe harbor has the potential to remove a real or perceived barrier to donations of cybersecurity technology and better address the growing threat of cyberattacks.

As we understand the rule today, any donation of valuable technology or services to physicians or other sources of federal health care program referrals can pose risks of fraud or abuse that may increase as the value of the donated technology rises. However, as technology constantly evolves at a rate that is difficult to keep pace with, the healthcare ecosystem has never been in more dire need for updates to these rules, to ensure the wider availability of appropriate levels of cybersecurity technology and proper protection of patient health information and other sensitive information.

The urgency is heightened due to the growing availability of patient health information. As more data exchange is encouraged and enabled, the adoption of robust cybersecurity solutions should be encouraged to effectively promote the continued flow of information as well as the evolving interoperable capabilities of EHR and other health information technology. The confidentiality, integrity, and availability of patient health information must be prioritized as a prerequisite to greater interoperability, and the expansion of these safe harbors helps put the healthcare sector on that path.

As the interoperability regulations from CMS and the Office of the National Coordinator for Health IT (ONC) move toward final, all federal agencies must appropriately align regulatory policy to allow more robust cybersecurity solutions to reach a larger number of providers in all care settings. As noted in the Proposed Regulation, "cyberattacks pose a fundamental risk to the healthcare ecosystem," and "data breaches can result in patient harm as well as high costs to the healthcare industry." HIMSS and PCHAlliance would argue that these threats come at a much higher cost than the perceived risk of accepting donated cybersecurity technology. In fact, cybersecurity solutions may be used to mitigate cybersecurity attacks and other types of cybersecurity compromises (e.g., due to insider threat). Cybersecurity and patient safety are directly connected. Patient safety cannot exist, unless data, devices, and other technology assets are kept safe and secure.

In addition, as some have described, the healthcare industry and the technology used to deliver healthcare are an interconnected ecosystem where the "weakest link" in the system can compromise the entire system. The monetary cost of acquiring and implementing cybersecurity solutions and related services has deterred some health system stakeholders who are unable to afford the expense from investing in adequate solutions. The ability to accept donations of these technologies and services is a reasonable allowance to address cost as an access issue, especially since many healthcare organizations spend only a fraction of their budget on cybersecurity solutions. Healthcare organizations need to maximize every dollar that is spent for cybersecurity solutions in addition to free government and industry resources such as the Health Industry Cybersecurity Practices (HICP).

A typical scenario is a small physician practice that is struggling to keep up with the pace of innovation and the adoption of new technologies to improve internal processes, empower patients, and deliver higher-value care. The cost of adopting appropriate

cybersecurity solutions are an added expense facing this practice that could be alleviated by granting this safe harbor.

Moreover, HIMSS and PCHAlliance support OIG's position to not require recipients to contribute a portion of the donor's costs for cybersecurity items and services. Consistent with the Health Care Industry Cybersecurity (HCIC) Task Force and our own HIMSS Cybersecurity Survey, OIG recognizes that many providers do not have adequate resources, including personnel and/or budget, to significantly invest in the cybersecurity technology protected by this proposed safe harbor. We believe omitting a contribution requirement will allow providers with limited resources to receive protected cybersecurity donations while also using their own resources to invest in other technology not protected by the safe harbor, such as updating legacy technology that may pose a cybersecurity risk.

- *Definitions and conditions*

To ensure that the provider community understands this safe harbor and how to take advantage of it, HIMSS and PCHAlliance encourage OIG to provide examples of what is allowed as well as not allowed in any forthcoming guidance documents. Providers and donating organizations should have enough clarity to make the determination about whether they fall within the parameters of the safe harbor. OIG should plan to use official government websites and other readily available, and easily accessible, communication vehicles (i.e., Medicare payment manuals). Ongoing education will also be necessary as technology is continuously evolving and we would recommend involving the healthcare information and technology community as well as the broader cybersecurity community in ongoing dialogue around any expansive education efforts.

In the Proposed Regulation, OIG also calls for steps that allow for the flow of donated cybersecurity to occur without abuse, by focusing on the applicability of the exception for the technology and related services that are necessary and predominantly used to implement, maintain, or reestablish cybersecurity. This step ensures that donations are being made for the purpose of addressing the legitimate cybersecurity needs of donors and recipients. Core function must be to protect information by preventing, detecting, and responding to cyberattacks and helps delineate between the technology and services that may have multiple uses beyond cybersecurity.

The breadth of protected technology is also sufficient as included in the Proposed Regulation, described as "any services associated with developing, installing, and updating software; any kind of cybersecurity training services – such as how to use the cybersecurity technology, how to prevent, detect, and respond to cyber threats, and how to troubleshoot problems with the cyber security technology." However, HIMSS and PCHAlliance would support the proposed "deeming provision" for an added layer of clarity.

- *Alternative proposal for cybersecurity hardware (Risk Assessment)*

HIMSS and PCHAlliance endorse the optional alternative of performing a risk assessment for those providers who wish to obtain donated cybersecurity hardware. Cybersecurity hardware must be determined to be reasonably necessary based on a risk assessment

of its own organization and that of the potential recipient. This alternative is reasonable given that it is proposed as optional, and providers do not need to satisfy this step if they are not looking to have the hardware component covered. In addition, providers must meet all of the other threshold conditions of this overarching safe harbor related to donated cybersecurity technology to even proceed to consideration of this alternative.

Amend the Existing Safe Harbors for EHR Arrangements

HIMSS and PCHAlliance support the continuation of the EHR Safe Harbor that protects certain arrangements involving the donation of interoperable EHR software or information technology and training services.

- *Deeming provision textual clarification*

We also support the proposed textual clarification within the "deeming provision" as it relates to the interoperable condition. Current conditions require donated items and services to be interoperable and prohibit the donor from taking action to limit the interoperability of the donated item or service. While the general construct remains intact, the textual clarification requires that certification must be current as of the date of donation, as opposed to the software having been certified at some point in the past, but no longer maintaining certification on the date of donation.

- *Information blocking definition*

HIMSS and PCHAlliance support OIG's intention to align the definition of information blocking with the significant updates that are taking place through ONC's regulatory processes. The ONC NPRM would implement the statutory definition of "information blocking," define certain terms related to the statutory definition of "information blocking," and currently proposes seven exceptions to the information blocking definition. OIG's Proposed Regulation recommends modifications to align with these updates. We agree with the sentiment that the proposed conditions are not intended to change the overall purpose, but rather to further the goal of preventing problematic arrangements that lead to information blocking.

- *Amendment relating to cybersecurity*

OIG clarifies cybersecurity software and services have always been protected under the EHR Safe Harbor and uses the Proposed Regulation to modify its language to include certain cybersecurity software and services that "protect" EHRs. Currently, the safe harbor "protects EHR software or information technology and training services necessary and used predominantly to create, maintain, transmit, or receive EHRs." OIG proposes to modify this language to include certain cybersecurity software and services that "protect" EHRs as well. HIMSS and PCHAlliance support this textual clarification to add more precision around the ability of entities that donate EHRs to expressly include cybersecurity software and services to safeguard the technology and patient health information.

- *Sunset provision*

OIG no longer believes that once nationwide EHR technology adoption has been widely achieved, the need for a safe harbor for donations of such technologies will diminish. OIG is proposing to eliminate, or as an alternative extend, the sunset deadline based on that rationale. HIMSS and PCHAlliance strongly agree with this approach and reaffirm that the need for these donations will only continue to grow as technology advances, providers from other care settings seek EHR tools, and greater interoperability opens up even more exchange possibilities for value-based care delivery.

Focus the 15-Percent Recipient Contribution Requirement Only on Certain Providers

OIG requires that a provider pay 15 percent of the overall cost for donated EHR items and services. The working assumption is that cost sharing is an appropriate method to address some of the fraud and abuse risks inherent in unlimited donations of technology. HIMSS and PCHAlliance support a targeted exemption from the contribution requirement for certain providers, such as providers in rural or underserved areas, providers serving underserved populations, small providers (specifically sole practitioners or a practice with no more than 2 employed clinicians), tribal providers, and critical access hospitals.

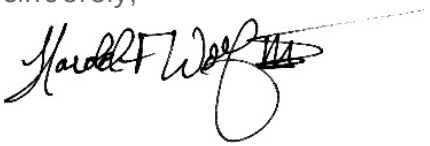
Overall, the data is clear that EHRs improve quality of care, patient outcomes, and safety, and more providers could benefit from utilizing this technology. The latest information from ONC (based on 2017 data), shows that nearly 80 percent of office-based physicians have a certified EHR system. Although 80 percent adoption is impressive, it means 20 percent of clinicians in private practice are not using certified EHR technology. As the financial burden that accompanies an EHR acquisition is a key challenge for more widespread nationwide adoption, we recommend that OIG use a targeted exemption from this requirement for those providers we deem as likely under-resourced—those from rural or underserved areas, serving underserved populations, small providers, Tribal providers, and critical access hospitals.

HIMSS and PCHAlliance remain committed to fostering a culture where health information and technology are optimally harnessed to transform health and healthcare by improving quality of care, enhancing the patient experience, containing cost, improving access to care, and optimizing the effectiveness of public payment.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact Ashley Delosh, HIMSS Senior Manager of Federal Affairs at adelosh@himss.org, or Robert Havasy, Managing Director of PCHAlliance at rhavasy@pchalliance.org, with questions or for more information.

Thank you for your consideration.

Sincerely,



Harold F. Wolf III, FHIMSS
President & CEO
HIMSS and PCHAlliance