December 26, 2019

Ms. Seema Verma
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
200 Independence Ave, SW
Washington, DC 20201

Dear Administrator Verma:

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 Program; Modernizing and Clarifying the Physician Self-Referral Regulations *(File Code: CMS-1720-P).* HIMSS and PCHAlliance appreciate the opportunity to leverage our expertise in offering feedback on the proposed exceptions to the physician self-referral law that focus on creating a new exception for donations of cybersecurity technology and related services, and an amendment to the existing exception for electronic health record (EHR) items and services.

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 physician self-referral statute was enacted to combat the potential that financial self-interest would affect a physician's medical decision-making and ensure that patients have options for quality care.

HIMSS and PCHAlliance support HHS' goal for two-sided risk, value-based arrangements to thrive in healthcare reimbursement models. However, to achieve that goal, it will be necessary for all evidence-based tools, including health technology, to be available to risk-based participants in value-based arrangements. The intent of this law is to prevent a physician from referring a patient for unnecessary services or to less convenient, lower quality, or more expensive health care, ultimately because the referring physician can improve his or her financial standing through those referrals. We find that the incentives for cost-control built into these two-sided risk, value-based arrangements will provide sufficient incentive for physicians to avoid steering patients towards lower-quality, higher-cost options.

As described in this Proposed Regulation, the CMS Physician Self-Referral Law proposal includes almost identical changes to the HHS Office of Inspector General Anti-Kickback Statute 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 Entities that Can Engage as a Value-Based Enterprise (VBE) Participant

HIMSS and PCHAlliance support and advocate for policy and practices that lead to the adoption of 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 evidence-based tools, including health technology, to be 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 incents those tools and services to improve care through better outcomes and lower costs.

HIMSS and PCHAlliance support 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.

Health technology companies and medical device manufacturers play an important role in care coordination and provide numerous types of digital and mobile health technology (like remote monitoring, data analytics, patient portals, and other communications). The broad exclusion of medical device manufacturers is likely to stifle 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 CMS evaluate and assess the complexities that would be involved with including these manufacturers as a VBE participant.

A full range of evidence-based tools and services is needed to make value-based enterprises successful. Full risk sharing that incents patient-centered, outcomes-driven care delivery can only flourish if all providers are able to access and use all these tools and practices.

If providers are 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. As a result, health technology will not be incented to deliver and innovate for improved outcomes and efficiency, leading to product development that does not drive toward value-based care.

Overall, we urge CMS to allow providers to share risk for outcomes with the developers and suppliers of the tools they believe will improve care and reduce costs. If all the requirements are satisfied, these exceptions should apply for value-based arrangements where a VBE has assumed full financial risk, a physician is incurring meaningful downside financial risk, as well as for indirect compensation arrangements for patient care services to a target patient population.

Create a New Exception for Donations of Cybersecurity Technology

HIMSS and PCHAlliance see the genuine need for an exception to protect arrangements involving the donation of certain cybersecurity technology and related services. We overwhelmingly support this major step forward, as it represents a fundamental acknowledgement that this exception has the potential to remove a real or perceived barrier to donations of cybersecurity technology and better address the growing threat of cyberattacks.

As the rule is interpreted 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 ensure the wider availability of appropriate levels of cybersecurity technology and proper protection of patient health information.

The urgency is heightened due to the growing accessibility of patient health information. As more data exchange is encouraged and enabled, the adoption of more cybersecurity controls should be encouraged to effectively promote the continued flow of information as well as the evolving interoperable capabilities of EHR technology. The integrity of patient health information must be prioritized when discussing greater interoperability, and the expansion of these exceptions helps put the community 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 cybersecurity to reach a larger number of providers in all care settings. In addition, as the risk of cyberattacks only continues to grow, HIMSS and PCHAlliance would argue that these threats come at a much higher cost than the perceived risk of accepting donated cybersecurity technology.

It is important to note, 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 technology and related services has deterred some health system stakeholders who are unable to afford the expense from investing in adequate measures. The ability to accept donations of these technologies and services is a reasonable allowance to address cost as an access issue.

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 measures is an added expense facing this practice that could be alleviated by granting this exception.

Moreover, HIMSS and PCHAlliance support CMS'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, CMS recognizes that many providers do not have adequate resources to significantly invest in the cybersecurity technology protected by this proposed exception. 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 exception, such as updating legacy hardware that may pose a cybersecurity risk.

- *Definitions and conditions*

To ensure that the provider community understands this exception and how to take advantage of it, HIMSS and PCHAlliance encourage CMS 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 exception. CMS 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, CMS 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 don't 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 exception related to donated cybersecurity even to proceed to consideration of this alternative.

Amend the Existing Exceptions for EHR Arrangements

HIMSS and PCHAlliance support the continuation of the EHR Exception 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 CMS'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. CMS'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*

CMS clarifies cybersecurity software and services have always been protected under the EHR Exception and uses the Proposed Regulation to modify its language to include certain cybersecurity software and services that "protect" EHRs. Currently, the exception "protects EHR software or information technology and training services necessary and used predominantly to create, maintain, transmit, or receive EHRs." CMS 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*

CMS no longer believes that once nationwide EHR technology adoption has been widely achieved, the need for an exception for donations of such technologies will diminish. CMS is proposing to eliminate, or as an alternative extend, the sunset deadline based on that rationale. HIMSS and PCHAlliance 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

CMS 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.

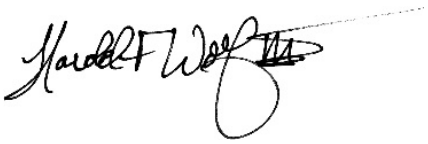
Overall, the data is clear that EHRs improve quality of care, patient outcomes, and safety, and more providers could benefit from utilizing this technology. The latest information from ONC (based on 2017 data), shows that nearly 80 percent of office-based physicians have a certified EHR system. Although 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 CMS 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 Jeff Coughlin, HIMSS Senior Director of Federal & State Affairs at jcoughlin@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