ConnectedHealthInitiative

February 9, 2026

The Honorable Thomas March Bell
Inspector General
Department of Health and Human Services
330 Independence Avenue SW
Washington, District of Columbia 20201

RE: Comments of the Connected Health Initiative regarding *Solicitation of Proposals for New and Modified Safe Harbors and Special Fraud Alerts (90 FR 57016)*

Dear Mr. Bell:

The Connected Health Initiative (CHI) writes to respond to the Department of Health and Human Services (HHS) Office of Inspector General's (OIG) annual solicitation of proposals and recommendations for developing new, or modifying existing, safe harbor provisions under section 1128B(b) of the Social Security Act, as well as developing new OIG Special Fraud Alerts.[1]

I. Introduction and Statement of Interest

The Connected Health Initiative (CHI) is the leading effort by stakeholders across the connected health ecosystem to clarify outdated health regulations, encourage the use of digital health innovations, and support an environment in which patients and consumers can see improvements in their health. We seek policy changes that will enable all Americans to realize the benefits of an information and communications technology-enabled healthcare system. For more information, see www.connectedhi.com.

II. Modernizing Enforcement of the Anti-Kickback Statute to Enable the Future Connected Care Continuum

Data from a variety of use cases demonstrates how connected health technologies available today improve patient care, prevent hospitalizations, reduce complications, and improve patient engagement, particularly for the chronically ill. These tools, including wireless health products, mobile medical device data systems, virtual care, telemonitoring-converged medical devices, and cloud-based patient portals, are revolutionizing American healthcare by securely enabling the exchange of health information and incorporating patient-generated health data (PGHD) into the continuum of care.

Over time, HHS has taken important steps to better utilize digital and connected health technology in several components of Medicare, such as through the expansion of support for remote patient monitoring in the Physician Fee Schedule, as well as in key Medicare program Alternative

[1] 90 FR 57016.

Payment Models (APMs) like the Medicare Shared Savings Program (MSSP). Despite the proven benefits of connected health technology to the American healthcare system, statutory restrictions and regulatory-level policy decisions inhibit the use of these solutions. As a result, utilization of digital health innovations is disconcertingly low, despite their ability to drastically improve beneficiary outcomes as well as generate immense cost savings.

CHI appreciates steps taken by HHS in recent years to advance the use of connected health innovations use, such as CMS' steps to support remote physiological monitoring (RPM) and remote therapeutic monitoring (RTM) by Medicare practitioners by clarifying that RPM is not part of the Medicare Telehealth Services list and is not subject to Section 1834(m) of the Social Security Act's restrictions. CMS has established its support for a modality-neutral approach to direct interactions between patients and providers through its support for RPM codes and is poised to further expand this approach through its approach to Chronic Care Management, Transitional Care Management, and Personal Care Management Services.

While important pro-digital health policy changes were made in the past, the pace of uptake for digital health innovations in the Medicare system continues to lag compared to the well-established benefits and efficiencies that cutting-edge technology offers. As a community, we continue to support OIG's efforts to utilize advanced technology to augment care for every patient via modernizing safe harbors. With the congressionally mandated shift from fee-for-service to value-based care in Medicare's approach, OIG efforts to improve its safe harbors, in coordination with other agencies, will be key in responsibly advancing the range of connected health innovations that will help American healthcare improve outcomes and reduce costs.

The healthcare system will not fully integrate these remote monitoring and virtual care technologies if current fraud and abuse regulations are not modernized. A continued leading impediment to the uptake of digital health tools across healthcare systems is the anti-kickback statute (AKS) and its restrictions that do not contemplate efficiencies provided by digital health technologies. CHI agrees that the AKS is an important anti-fraud protection for Medicare; however, it has not kept pace with change within the healthcare industry. Instead, it may present barriers to innovation, and it is critical that there are considerations for new safe harbors. Many technology companies provide substantial financial and in-kind resources to support innovative care models. Under current fraud and abuse regulations, it is unclear the extent to which technology companies can contract directly with providers and manufacturers to address Medicare patients' needs. Existing waivers under the AKS and civil monetary penalties (CMP) for value-based arrangements are limited to participants in the Medicare Shared Savings Program or Center for Medicare and Medicaid Innovation (CMMI) models. Many providers outside those programs would like to pursue opportunities to engage with technology companies to serve their patient populations. Because of OIG's strict interpretation of the statute, it is risky for technology companies to enter into agreements to subsidize the costs of certain interventions for providers, even where those services would be medically necessary to reduce future healthcare costs.

CHI notes that modernizing AKS safe harbors to accommodate digital health and AI innovations is consistent with the Administration's commitment to reducing regulatory barriers to innovation and cutting unnecessary bureaucratic impediments to healthcare delivery. Outdated fraud and abuse regulations that were designed for a fee-for-service, in-person care paradigm impose compliance costs and legal uncertainty that disproportionately burden the small and medium-sized technology companies that are driving healthcare innovation. OIG's safe harbor modernization effort presents an opportunity to advance deregulatory objectives while maintaining robust protections against actual fraud and abuse, a balance that can be achieved

by focusing enforcement on conduct rather than categorical exclusions of entire industry segments from safe harbor eligibility.

III. CHI's Recommendations for the OIG's New Safe Harbors and Special Fraud Alerts

Generally, CHI supports the creation of AKS safe harbors that will responsibly facilitate greater acceptance and use of connected health innovations—be they hardware, software, or a combination of the two—throughout the continuum of care. We offer the following specific input on OIG safe harbors and special fraud alerts:

a. OIG Safe Harbors Should Enable All Entities that Facilitate Value-Based Care to Qualify as a "Value-Based Enterprise"

While the traditional value-based enterprise (VBE) is envisioned with clinicians, providers, or suppliers, we support digital health companies also being eligible for participation as a VBE due to their investment in and work surrounding the implementation of connected health technologies. Vendors of digital health technologies and services add significant value as VBE participants through their data analytics capacity and ability to access resources that are unattainable to many provider entities. The creation of innovative business arrangements that include digital health companies as active participants who can share in risk has the potential to significantly move the needle and create improved outcomes at overall reduced costs. CHI recognizes that digital health technology companies' arrangements will still need to meet all existing safe harbor requirements. However, by broadening the definition of a VBE, more patients will be able to benefit from a clinician, provider, or supplier entities' relationship with digital health companies, which will in turn improve patient outcomes.

Noting our support for including companies that make mobile health and digital technologies in the scope of a VBE entity, CHI strongly urges OIG to ensure that it does not exclude countless Americans from the benefits of connected care, consistent with HHS' goal of enhancing a connected care continuum including, but not limited to, the provider setting. We believe that OIG shares our concern based on its past acknowledgement that OIG's definition of a "medical device manufacturer" should not inadvertently limit the availability of the mobile and digital health technology that would provide benefit to value-based arrangements.

CHI notes that companies producing medical devices (either software, hardware, or some combination or the two), including Durable Medical Equipment, Prosthetics, Orthotics, & Supplies (DMEPOS) manufacturers, play a significant and frontline role in providing for a fully connected care continuum that includes different settings outside of the provider's location. These technologies include—but are not limited to—patient portals that provide data analytics and remote patient monitoring systems, which are essential ingredients to effective and efficient care coordination through monitoring real-time patient data for those diagnosed with disease, as well as in the early detection and prevention of disease. We urge OIG to reduce confusion that would be caused by its declaration that pharmaceutical and DMEPOS manufacturers and laboratories are "less likely to be on the front line of care coordination and treatment decisions" by updating its discussion to reflect the role these entities play in today's care coordination.

The connected health technology market is rapidly evolving, with a melding of traditional categorizations within the medical industry taking place due to startups identifying new market niches, acquisitions, etc. Under OIG's current rule, many CHI members find themselves potentially classified as medical devices, DMEPOS manufacturers, and/or pharmaceutical manufacturers. This will result in further inconsistency with congressional intent for the AKS and the Physician Self-Referral Law that focuses on conduct rather than organizational categorization.

Rather than unequivocally excluding industry categorizations from being VBE participants, OIG, through its safe harbors, should instead not exclude any certain entities from this scope and should focus its rules on behavior representing fraud and abuse in violation of the AKS. This approach would be consistent with many of the proposed safe harbors in OIG's proposed rule addressing marketing (e.g., requiring a prescription for use of a certain technology in a value-based arrangement) and clinical decision-making (e.g., allowing physicians to select technology from outside of the value-based arrangement if appropriate), among others. CHI believes that appropriate reporting and transparency requirements from the value-based arrangement, paired with objective enforcement, can largely make these safeguards feasible.

b. OIG Should Waive Cost-Sharing Requirements for Connected Health Technologies

CHI stakeholders' experiences clearly demonstrate patient cost-sharing requirements to be a barrier to the uptake of connected health technologies used for care management and RPM. We support OIG providing for the waiver or offset of cost-sharing obligations for care management and RPM use cases where the cost-sharing waiver or offset of obligations is part of a value-based arrangement, particularly where the costs of collection exceed the amount to be collected, with reasonable and objective fraud and abuse measures.

CHI recognizes OIG's concerns regarding RPM/RTM billing integrity, as reflected in OIG's August 2025 report identifying potentially suspect RPM/RTM billing patterns and its ongoing audit activities. We share OIG's commitment to safeguarding the Medicare program from fraud, waste, and abuse. We emphasize that well-designed safe harbors can actually support enforcement by drawing a clear line between legitimate, beneficial RPM/RTM arrangements and abusive schemes. Providers and technology companies operating in good faith need regulatory certainty, and the absence of clear safe harbor protection paradoxically allows bad actors to thrive while discouraging compliant innovators from entering the market.

c. OIG Should Exempt its Durable Medical Equipment Annual Certification Requirement for Remote Patient Monitoring

CHI urges OIG to ensure that DMEPOS enabled by internet connectivity and new, innovative features be permitted to meet CMS' requirement for face-to-face encounters. Care providers can leverage connected health technology to obtain Durable Medical Equipment (DME) PGHD for continual evaluation and treatment of conditions. Such capabilities negate the need for an annual demonstration of medical necessity through their ongoing collection and transmission of PGHD. Therefore, CMS should mitigate or eliminate, through safe harbors, this annual certification requirement when remote patient monitoring tools, whether physiologic or therapeutic, can demonstrate medical necessity.

d. OIG Should Enable Patient Access to Digital Health Equipment and Software Platforms

As clinicians remotely monitor patients at home who may have acute and chronic conditions, there are ongoing concerns that any equipment or access to software platforms provided free of charge may inadvertently trigger liability under the AKS. CHI requests that OIG clarify that providing access to software-based platforms for PGHD analytics or telemedicine at no/low cost does not violate the AKS. Additionally, the operative definition for "remuneration" in this statutory provision, at 42 U.S.C. 1320a–7a(i)(6), is broad, and we recommend that the OIG also provide clear guidance that giving patients a device to communicate with a care team is not considered a beneficiary inducement. These clarifications will enable the provisioning of RPM, telehealth, and other tech-driven healthcare tools without triggering AKS liability.

e. OIG Should Enable Access to Devices with Multiple Functions to Reflect Modern Use of Digital Health Tools in Care Delivery

We call on OIG to clarify that utilization of a device with multiple functions, such as a smartphone or e-tablet, does not violate the AKS and the CMP when it is primarily used for managing a patient's healthcare, including the social determinants—e.g., finances, scheduling, and transportation—that affect a patient's health. Multifunction devices are essential to the successful and responsible application of connected health technology to improve outcomes and reduce costs. However, many existing interpretations of the AKS regulations and guidance prohibit such devices from reaching the patients who need it most. Multi-function devices offer the ability in clinical trials to validate the identity of trial participants and allow healthcare functionality to be integrated into the other digitized aspects of a patient's life, such as their email and text message communications, personal finances, or navigation, making patients more likely to use a multi-function device, while also giving providers real-time information about a patient's status (e.g., blood pressure or heart rate).

f. OIG Should Clarify the Applicability of the Anti-Kickback Statute to Artificial Intelligence

HHS and the CHI community continue to assess how best to implement, integrate, and regulate the role of artificial intelligence (AI) in healthcare. As part of this ongoing effort, CHI encourages OIG to collaborate with its HHS counterparts and our community to evaluate and provide guidance on the application of the Anti-Kickback Statute to the use and funding of AI technologies. As a prime example, in the context of clinical trials and drug development, manufacturers providing AI or digital health technologies to individual providers—intended to assist in identifying clinical trial treatment options for their patients—could be interpreted as a kickback or a violation of the False Claims Act. Existing OIG compliance guidance has indicated that recruitment bonuses should only be offered to researchers (not to physicians identifying trial participants) and must be tied to additional efforts made to recruit participants. While the use of AI technology to improve clinical trials, lower prohibitive costs, and accelerate the development of critical new drugs and devices does not directly conflict with the Anti-Kickback Statute or previous compliance guidance, CHI believes that explicit clarification is needed. Specifically, guidance that acknowledges innovative approaches in trial design and execution—such as enabling physicians to use AI technology to identify potential trial participants—would provide much-needed clarity. Therefore, CHI urges OIG to work closely with stakeholders to clarify how relevant statutes apply and, where appropriate, establish explicit safe harbor exceptions for alternative financing models involving AI technology.

Further, since CHI last addressed this topic with OIG, the rapid proliferation of generative AI and large language models (LLMs) in healthcare has introduced additional novel AKS questions requiring OIG attention. Generative AI tools are now being deployed for clinical documentation, ambient listening, clinical decision support, prior authorization processing, and care coordination workflows. When an AI vendor provides a free or subsidized AI-powered tool, such as a clinical documentation assistant or an ambient scribe, to a provider practice, it is unclear whether such arrangements constitute remuneration that could trigger AKS liability. Similarly, AI-driven care coordination platforms that aggregate and analyze patient data across multiple providers raise questions about the scope of permissible technology-sharing arrangements. CHI urges OIG to develop specific guidance or safe harbor protection addressing the provision of AI-enabled tools in clinical settings, particularly where such tools are designed to improve care quality, reduce administrative burden, and lower costs. OIG's Advisory Opinion 25-03, addressing telehealth collaboration structures under the personal services safe harbor, demonstrates the type of clarity needed, but advisory opinions are fact-specific and do not provide the broad protection that formal safe harbor regulations would deliver.

Further, CHI has worked with the broader community to develop healthcare ecosystem-wide consensus recommendations on the use of AI in healthcare, which generally encourage OIG to align with:

- CHI's *Health AI Policy Principles*, a comprehensive set of recommendations on the areas that should be addressed by policymakers examining AI's use in healthcare, and how they should be addressed (https://connectedhi.com/wp-content/uploads/2022/02/Policy-Principles-for-AI.pdf);
- CHI's *Advancing Transparency for Artificial Intelligence in the Healthcare Ecosystem*, a proposal on ways to increase the transparency of and trust in health AI tools, particularly for care teams and patients (https://connectedhi.com/wp-content/uploads/2022/02/AdvancingTransparencyforArtificialIntelligenceintheHealthcareEcosystem.pdf); and
- CHI's *Health AI Roles & Interdependency Framework*, which proposes clear definitions of stakeholders across the healthcare AI value chain, from development to distribution, deployment, and end use; and suggests roles for supporting safety, ethical use, and fairness for each of these important stakeholder groups that are intended to illuminate the interdependencies between these actors, thus advancing the shared responsibility concept (https://connectedhi.com/wp-content/uploads/2024/02/CHI-Health-AI-Roles.pdf).

g. OIG Should Expand Cybersecurity Safe Harbor Protections for Connected Health Infrastructure

The 2020 Final Rule included a cybersecurity technology and services safe harbor, recognizing the critical importance of robust cybersecurity in healthcare. As the deployment of connected health devices, RPM/RTM systems, and AI-enabled tools accelerates, the cybersecurity infrastructure required to support these technologies has grown substantially. CHI recommends that OIG expand or develop new cybersecurity safe harbor protections specifically addressing the security infrastructure necessary for RPM/RTM and connected health deployments. This should include protections for technology companies that provide cybersecurity tools, threat monitoring services, and security training to provider organizations as part of connected health

arrangements, where such provision is designed to protect patient data and ensure the integrity of remote monitoring and virtual care systems.

IV. Conclusion

We appreciate the opportunity to provide input on the OIG's solicitation of new safe harbors and special fraud alerts as it begins to develop new regulations.

Sincerely,

Brian Scarpelli
Executive Director

Chapin Gregor
Policy Counsel

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005