AdvaMed
Advanced Medical Technology Association

October 27, 2025

By Electronic Submission to www.regulations.gov

Ms. Stacy Murphy
Deputy Chief Operations Officer and Security Officer
Office of Science and Technology Policy (OSTP)
Executive Office of the President
1650 Pennsylvania Avenue NW
Washington, DC 20504

Re: Docket No. OSTP-TECH-2025-0067, Notice of Request for Information; Regulatory Reform on Artificial Intelligence, 90 Fed. Reg. 46422 (Sept. 26, 2025)

Dear Deputy Chief Murphy:

The Advanced Medical Technology Association (AdvaMed) appreciates the opportunity to submit comments in response to your September 26, 2025, request for information (RFI) on priorities for such regulatory reform or other agency action necessary to promote AI innovation and adoption.[1]

AdvaMed is the world's largest association representing manufacturers of medical devices, diagnostic products, and medical technology. AdvaMed's member companies range from the largest to the smallest medical product innovators and manufacturers, with nearly 70 percent of our members generating less than $100 million in annual sales. AdvaMed's member companies produce innovations that transform healthcare through earlier disease detection, less invasive procedures, and more effective treatments. AdvaMed advocates for a legal, regulatory, and economic environment that advances global healthcare by assuring worldwide patient access to the benefits of medical technology. The Association promotes policies that foster the highest ethical standards, timely product authorization, appropriate reimbursement, and access to international markets.

We recognize AI as a transformative tool with the potential to improve health outcomes, enhance the efficiency of patient care, reduce costs, and advance healthcare. Right-sized and clarified regulations can promote the development, deployment, and adoption of innovative and trustworthy AI-enabled solutions. AdvaMed is uniquely well-positioned to provide feedback on frameworks and policy considerations for AI, as our members have been developing and deploying AI-enabled medical devices that support patient

[1] https://www.federalregister.gov/documents/2025/09/26/2025-18737/notice-of-request-for-information-regulatory-reform-on-artificial-intelligence.

care for over 25 years.

We appreciate the opportunity to submit our high-level recommendations on priority opportunities for regulatory reform needed to sustain and enhance AI innovation in the medical device industry.

I. USE OF AI AND SOFTWARE-BASED TECHNOLOGIES IN THE MEDICARE PROGRAM

Leaders of this Administration have been outspoken on their concern for the poor health outcomes in the United States despite the abundant resources at our disposal. AdvaMed and the broader medtech community share this deep concern. We also know medtech is a proven part of the solution. Medtech works. But it only works if patients have access to it and clinicians are empowered to use it. Access is complicated by many factors: inadequate or no health insurance coverage; lack of provider coverage of medtech-enabled procedures; inadequate provider reimbursement for medtech-enabled procedures; limited access to specialists and care due to factors including geography and health care provider shortages; limited understanding of available treatment options; and other out-of-pocket expenses associated with health care, such as high deductibles and copayments.

As you know, the Centers for Medicare and Medicaid Services (CMS) plays a critical role in patient access to health care and medtech. Medicare, as the nation's largest health insurer, shapes the health of its 67 million enrollees. It sets precedent in its coverage policies for Medicaid and private insurers. Unfortunately, outdated Medicare laws and regulations often create unnecessary barriers to patient access to many technological innovations, including artificial intelligence and other items and services, along with digital and at-home care.

Adoption of and subsequent beneficiary access to novel digital health technologies is conditioned on whether there are appropriate Medicare payment pathways that provide stability and certainty for providers adopting these technologies. While CMS has explored payment policies to recognize the role of software as a service (SaaS), software as a medical device (SaMD), and AI technologies in health care delivery, a lack of clear and consistent coverage and payment policies for these technologies significantly limits access under the Medicare program. AdvaMed members are on the front lines of innovation in this space, and we appreciate the opportunity to provide comments and serve as a resource to this administration as it continues to explore expanding patient access to AI and software-based technologies.

Our comments below address the following:

- Ensuring Consistency in Medicare Terminology Regarding Digital Health Technologies
- Securing Coverage and Payment for Digital Health Technologies Under Medicare's Payment Systems
- Additional Considerations

A. Ensuring Consistency in Medicare Terminology Regarding Digital Health Technologies

First, we encourage CMS to clearly and consistently name and define the technologies that would be impacted by future payment policy proposals. While the agency utilizes "SaaS" through the comment solicitation, we believe SaMD would be a more accurate description of technologies involved in the clinical delivery of care.[2] SaMD directly impacts the diagnosis or treatment of patient disease, has ancillary costs just like any other medical service paid for under a Medicare payment system, and involves clinician interaction with the technology and the individual patient during care delivery and interpretation of results. Definitions that are standardized and consistently applied will allow CMS, FDA, and other key stakeholders to work collaboratively as SaMD payment policy is developed and implemented.

Because of its role in patient care, it is imperative that any payment policy clearly delineate between FDA-regulated and unregulated digital health technologies. Unlike unregulated digital health technologies, such as wellness apps, SaMD are subject to the same regulatory oversight by the FDA as hardware medical devices. The legal, regulatory, and financial burdens of developing SaMD are no less stringent than those of manufacturing hardware medical devices.

We further encourage the Agency to ensure appropriate coding solutions are in place for all procedures that utilize SaMD to ensure patients can access these treatments, and to work with stakeholders in this process.

B. Securing Coverage and Payment for Digital Health Technologies Under CMS' Payment Systems

1. Hospital Outpatient Prospective Payment System (OPPS)

(a) New Technology Ambulatory Payment Classification (APC) Improvements

In the CY 2023 OPPS/ASC final rule, CMS established a policy for the separate payment of SaaS add-on codes, excluding SaaS from the packaged payment policy at 42 CFR 419.2(b)(18). We are greatly encouraged by CMS acknowledging the uniqueness of these technologies, and recognizing the need for separate payment and consideration of these services. As CMS recognized in the CY 2023 OPPS/ASC final rule, the number of such services undergoing FDA review has and will continue to increase rapidly. We encourage CMS to provide much-needed stability and certainty regarding SaaS by formalizing the exception to the packaged payment policy in regulatory text. We further recommend that CMS establish a dedicated section of the OPPS rule to SaMD and related technologies moving forward, as opposed to limiting discussion and consideration of these services within the New Technology APC section of the preamble text.

Beyond the current SaaS pathway, we believe additional changes are needed to ensure appropriate

[2] The term "algorithm based healthcare services" (ABHS) has also been used by AdvaMed in other communications to CMS and is referenced in The Health Tech Investment Act (S.1399), pending before Congress.

payment systems are in place for novel SaMD, including algorithm-based healthcare services (ABHS)[3]. We therefore offer the following three recommendations.

First, we ask the agency to revise the New Technology Ambulatory Payment Classification (APC) application process for these FDA-regulated, software-based interventions. The application process should be tailored to the unique characteristics of these technologies, while staying true to the policy priorities CMS established as part of the current New Technology APC application requirements (including the creation of procedural C-codes as needed). As an example, the application should reflect the impact of a SaMD on care pathways and how these services assist practitioners in the delivery of care.

Second, we encourage CMS to modify the current New Technology APC policies as they relate to SaMD both currently assigned to a New Technology APC and for future technologies (including via a potential New Technology APC for SaMD application pathway). Specifically, we recommend CMS: (1) provide stability for SaMD developers by assigning these technologies to a New Technology APC for at least five years; and (2) waive the Universal Low Volume APC policy for these technologies when assigned to a New Technology APC. Both recommendations are intended to ensure stability during the New Technology APC period. As it relates to the five-year price stability period, we note this would align with the lifespan of a Category III code and is necessary to ensure appropriate data collection and analysis can occur while hospitals adopt novel SaMD. Further, the five-year stability is intended to ensure there are not variations in New Technology APC assignment based on misreported or omitted cost information. In recent years, including the CY 2024 OPPS/ASC final rule, we have seen how the existing policies create payment aberrations that pose serious threats to the adoption of these novel SaMD, such as confusion among adopters and a chilling effect on innovation.

Third, we urge CMS to be proactive in considering clinical APC assignments for SaMD. While some technologies can be appropriately assigned to an existing clinical APC, CMS should begin to consider policy options for future SaMD that may not meet the criteria for assignment to current clinical APCs. In recognition of the continual evolution of SaMD, we urge CMS to continue to work with developers to ensure these technologies can be appropriately transitioned out of New Technology APC payments after five years and be assigned to an appropriate clinical APC.

(b) Transitional Pass-Through Payment (TPT) Improvements

Under TPT and the new technology APC policies for eligible new devices, CMS provides higher payments to aid with the uptake by hospitals of eligible new medical devices. The current TPT criteria specifically require that a device must —

[3] ABHS are clinical analytical services delivered by FDA-cleared devices to a healthcare practitioner that use artificial intelligence, machine learning, or other similarly designed software to produce clinical outputs for the diagnosis or treatment of a patient's condition. ABHS provide quantitative and qualitative analyses, including new, additional clinical outputs that detect, analyze, or interpret data to improve screening, detection, diagnosis, and treatment of disease.

- Be an integral part of the service furnished;
- Be used for one patient only;
- Come in contact with human tissue; and
- Be surgically implanted or inserted (either permanently or temporarily) or applied in or on a wound or other skin lesion.

Furthermore, the device cannot be any of the following:

- Equipment, an instrument, apparatus, implement, or item of this type for which depreciation and financing expenses are recovered as depreciable assets; or
- A material or supply furnished incident to a service (for example, a suture, customized surgical kit, scalpel, or clip, other than a radiological site marker).

As AI and SaMD are increasingly introduced for more and more procedures and frequently include components that do not come into contact with patients or represent a capital expenditure, these criteria are inappropriately exclusionary for these technologies. In particular, because capital costs are included in establishing the APC payment rate, the same rationale applies equally when calculating the operating costs for pass-through payments. We therefore urge CMS to consider improvements to the TPT program allowing SaMD and other technologies that do not come into contact with patients to be eligible for additional payments under this program.

2. Physician Fee Schedule

We encourage CMS to consider holistic updates to its fee-for-service payment systems to reflect the significant resource investments required to adopt and implement not only SaMD, but the broader scope of workflow and process improvement software and related technologies. These investments extend beyond the procurement of a software license and include cybersecurity updates, staff training, and hardware procurement. While these costs are typically considered indirect and therefore not reimbursable, we encourage the agency to consider how they might be incorporated into annual market basket updates or other update factors to ensure appropriate accounting for provider costs. Given the new and innovative nature of SaMD, we recommend CMS consider payment policies that are harmonized across payment systems and reflect that many of these technologies may lack historical claims data. As one option, CMS may consider utilizing G codes for supply of SaMD and the associated monitoring. This approach, which the agency has already similarly implemented in its DMHT payment policy, would apply to SaMD that have an FDA indication, have undergone rigorous clinical and safety reviews, and include quality controls. The physician could procure the license, prescribe to the patient, and receive reimbursement. We believe approaching SaMD as a supply with contractor pricing may be one way to introduce a consistent payment policy for these technologies while recognizing the varied and extensive SaMD technology landscape until such time that an appropriate national rate could be established.

In addition to bringing consistency to payment, this approach would further allow CMS to recognize the

critical and distinct value of the different types of SaMD. Technologies designed for chronic care management, preventative care, and early diagnosis are all vastly different with varying costs and substantial potential value for patients, clinicians, and the health care system. We encourage the agency to implement payment policies that reflect the diversity of individual SaMD and the collective benefits these technologies offer.

3. Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) Fee Schedule

The DME benefit category can be used for certain SaMD that meet the regulatory definition of DME. However, the current definition creates significant barriers to access under this program. We strongly recommend CMS revise its DME regulations to provide more specific direction for how digital therapeutic software technologies can be covered and paid under the program by:

- Clarifying DME coverage policies to reflect how digital therapeutics can be covered as DME;
- Revising accreditation standards for the special characteristics of SaMD;
- Aligning payment policy with the duration the SaMD technology is intended to be used;
- Ensuring distribution flexibility that supports patient access, understanding that transfer of title is not always appropriate or desired for these products; and
- Clarifying how the requirements within the statutory definition of DME apply to SaMD (e.g., recognizing that some digital therapeutic devices, which are regulated by the FDA as SaMD, have a three-year extended life but may not be appropriate for use by multiple individuals and thus may not be appropriate for rental).

4. Devices that Streamline Operations while Improving Outcomes

We recommend that CMS consider alternative payment pathways for AI-enabled capital that can substantially reduce waste, enhance workflow efficiencies, and improve patient quality, including through medication management. Though inpatient settings may have historically conducted these internal value assessments, post-acute facilities, including Skilled Nursing Facilities and Behavioral Health settings, are limited in their capacity to adopt new technologies. We recommend that CMS work with industry, hospital, and pharmacy leaders to envision operational and clinical excellence with a reimbursement pathway to incentivize it.

C. Additional Considerations

Despite the advancements in prevention, treatments, and therapies, challenges to access and disparities in care persist in the US health system. Factors such as geographic inaccessibility, economics, insurance, QHP shortages, health system bias, race and ethnicity, language and many other factors contribute to this growing trend. In addition, for many conditions, access to evidence-based first-line therapy is limited at

best, reducing care quality, negatively impacting population health, and increasing total health care costs. The very nature of SaMD provides opportunities to achieve access to evidence-based care at scale, especially for underserved populations. These innovative technologies are proven to deliver clinically effective treatment and allow for ongoing care to reach health care deserts where access to QHPs is challenged and where existing treatments fall short.

In addition to the SaMD recommendations discussed above, we encourage CMS to consider holistic updates to its fee-for-service payment systems to reflect the significant resource investments required to adopt and implement not only SaMD, but the broader scope of workflow and process improvement software and related technologies. These investments extend beyond procurement of a software license and include cybersecurity updates, staff training, and hardware procurement. While these costs are typically considered indirect and therefore not reimbursable, we encourage the agency to consider how they might be incorporated into annual market basket updates or other update factors to ensure appropriate accounting for provider costs.

II. REGULATORY

FDA has a comprehensive regulatory framework that ensures the safety and effectiveness of many different types of medical devices across the product's lifecycle. FDA's oversight is guided by a risk-based framework that includes a rigorous premarket review process as well as extensive post-market monitoring requirements after devices are authorized for sale. FDA's regulatory frameworks are applicable to a broad array of medical devices and are designed to accommodate emerging technologies in medical devices, such as AI. FDA has been regulating AI-enabled medical devices for over 25 years and, as of July 10, 2025, the FDA has authorized over 1,200 AI-enabled devices. As discussions about oversight of AI technologies across industries continue to evolve, it is crucial to ensure that regulations are tailored to address the respective challenges and opportunities AI presents in different sectors. Therefore, FDA should remain the sole regulator overseeing the safety and effectiveness of AI-enabled medical devices. FDA oversight ensures that safety and performance considerations unique to AI-enabled medical devices are evaluated and regulated with the appropriate context and rigor.

The FDA's premarket review of AI-enabled devices includes, among other considerations, an assessment of the safety testing and performance validation conducted by device manufacturers, an assessment of the conducted risk analysis, and an assessment of the mitigation of unwanted bias for the intended patient population. The FDA's regulatory oversight continues in the post-market part of the device's lifecycle, with requirements for manufacturers to conduct ongoing monitoring and reporting of device performance and safety to mitigate risks and ensure compliance with regulations. FDA guidance can enhance transparency and clarify regulatory expectations. FDA's expectations for both the pre- and post-market have been outlined in its draft guidance titled, "Artificial Intelligence-Enabled Device Software Functions: Lifecycle

Management and Marketing Submission Recommendations[4]." We commend FDA for the timely issuance of this draft guidance, however, the recommendations therein are intended to apply broadly to all types of AI and apply a one-size-fits-all approach. Guidance is most effective when the recommendations are right-sized and adhere to the Agency's least burdensome principles[5]. FDA should update the guidance and regularly collaborate with stakeholders to ensure the recommendations accurately reflect the needs and nuances of the technology. As AI technology matures, international consensus standards specific to medical devices should be the foundation for safe, effective, and responsible development, deployment, and monitoring. It is critical that FDA prioritize the development, revision, and timely recognition of such standards to promote industry-wide adoption of these best practices.

In 2022, Congress passed predetermined change control plan (PCCP) legislation. PCCP is an innovative concept that is intended to enable regulatory efficiency because it permits a manufacturer to make controlled changes or updates to a device in accordance with the FDA-authorized PCCP without needing to submit a new premarket submission to FDA. The PCCP authority enables manufacturers to innovate more efficiently and rapidly to help improve patient health while still ensuring the safety and effectiveness of the device. The PCCP framework is broadly applicable to all medical devices but is particularly valuable to AI-enabled devices as it enables the FDA's regulatory frameworks to keep better pace with the rapid innovation inherent to AI, and ensures clinicians and patients have timely access to improved devices. To fully realize these benefits, it is essential that FDA's implementation of the PCCP framework continues to evolve in step with the accelerating advancements in AI.

III. DATA PRIVACY

Access to high-quality data is pivotal AI model development and validation. Updating data regulatory frameworks, such as HIPAA, to facilitate ethical and secure data-sharing practices will further enhance the development of sophisticated AI tools.

AI Researchers require improved access to healthcare data that is both rich enough to support meaningful scientific development and sufficiently de-identified to protect patient privacy from wrongful disclosure or abuse. Policymakers can support advances in healthcare AI innovation by allowing broader use of healthcare data for research, provided identifiers are removed and other HIPAA rules are met (e.g., HIPAA's security requirements and its limitations on "selling" or marketing without prior written permission).

In parallel, a broad, prospective informed consent framework would enable individuals to contribute their data to a centralized repository for future research, enabling reuse across studies and institutions.

---

[4] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/artificial-intelligence-enabled-device-software-functions-lifecycle-management-and-marketing

[5] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/least-burdensome-provisions-concept-and-principles

A. "Health Care Operations" under HIPAA

We recommend amending the definition of "health care operations" at 45 CFR § 164.501 to explicitly include AI model development and validation for the delivery, management, or improvement of health care services, with appropriate guardrails. The current definition of health care operations permits a HIPAA covered entity to perform specified activities without individual authorization, including "conducting quality assessment and improvement activities . . . provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities." Where the primary purpose of such activities is obtaining generalizable knowledge, the activity would instead be categorized as research, as defined at 45 CFR § 164.501. However, as HHS itself has recognized, the distinction between quality assessment and improvement activities and research can be unclear. This is often the case in the context of product innovation, where the line between health care operations-type improvements and research and development can be difficult to discern. When evaluating activities that fall within this gray area, covered entities must choose between following HIPAA's research rules, which require the entity to obtain certain permissions and take additional compliance steps, thereby delaying initiation of the activity, or risking enforcement exposure if a regulator disagrees with the covered entity's conclusion that the activity qualifies as health care operations.

Proposed language: Amend paragraph (1) of the definition of "health care operations" in 45 CFR § 164.501:

> ***Health care operations*** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
>
> (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; AI model development and validation for the delivery, management, or improvement of health care services; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.

The proposed modifications would help provide certainty to covered entities that encounter this ambiguity when developing and improving AI models used for specified health care purposes. It would also enable them to fast-track AI innovations by not subjecting lower-risk activities to the burdensome HIPAA research rules. In addition, with its purpose limitation, including by extending health care operations model development only to internal activities, the proposal maintains protections for individuals, requiring compliance with existing HIPAA rules where protected health information (PHI) is sought to be used for other purposes.

B. HIPAA De-Identification Safe Harbor Flexibility

We recommend enhancing the flexibility of the de-identification standard at 45 CFR § 164.514 by allowing Safe Harbor de-identified datasets to retain otherwise restricted indirect identifiers that are important for AI development. HIPAA provides two means through which PHI may be de-identified. The first is the Safe Harbor method, which requires the removal of specified data elements and the absence of actual knowledge that the remaining information can be used to identify an individual. The second requires a formal determination from a qualified expert that, based on an analysis meeting certain criteria, the risk of re-identifying an individual in the dataset is very small. Once data has been de-identified under either method, it is no longer subject to HIPAA's restrictions on the use and disclosure of PHI. This makes HIPAA de-identified data valuable for various purposes, including AI product development and training.

The Safe Harbor method is generally easier to apply, as it does not require specialized knowledge that most organizations do not have in-house. This allows internal teams to de-identify data as needed in the regular course of their operations. The expert determination method, however, usually requires organizations to engage a third-party expert, which demands valuable time, money, and other valuable resources. Notwithstanding, many organizations are forced to rely on the expert-determination method, given its flexibility, which provides a pathway to creating and using more valuable de-identified datasets. Under that method, an expert can deem a dataset as de-identified, even if it has data elements that could not be included under the Safe Harbor, provided the expert's analysis meets HIPAA requirements. Dates related to individuals (e.g., date of service) and zip codes are examples of data elements that HIPAA-regulated entities often identify as valuable for product development that must be excluded from a Safe Harbor de-identified dataset, and that often are approved through expert determinations.

Proposed language: Amend 45 C.F.R. § 164.514(b)(2) by adding paragraphs 45 C.F.R. § 164.514(b)(2)(iii) and (iv):

(b) ***Implementation specifications: Requirements for de-identification of protected health information.*** A covered entity may determine that health information is not individually identifiable health information only if:

. . .

(2) (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including

birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(iii) Notwithstanding paragraphs (b)(2)(i) and (b)(2)(ii) of this section, a covered entity may determine that health information is not individually identifiable if it contains identifiers described in paragraph (b)(2)(iv), provided that the dataset contains only the minimum necessary of such data elements required for a specific AI development or training use case, is used only for such purposes, and the covered entity complies with paragraph (b)(2)(ii).

(iv) Identifiers listed in paragraphs (b)(2)(i)(B) and (b)(2)(i)(C) may be included in a de-identified dataset, in accordance with paragraph (b)(2)(iii).

The proposal seeks to relieve the burden on HIPAA-regulated entities from needing to rely on expert determinations to create valuable de-identified datasets for model development and training. This would allow those entities to dedicate more resources toward efficiently creating and improving AI-enabled products that can enhance the experience and outcomes of patients and consumers, while mitigating potential risks associated with the re-identification of individuals in de-identified datasets. Under the proposal, only the minimum necessary indirect identifiers would be permitted in a Safe Harbor de-identified dataset, as required by the circumstances of a particular use case.

C. Use of AI to Process PHI for Treatment, Payment, or Health Care Operations

We recommend clarifying that it is permissible to process the minimum necessary PHI through a third-party generative AI tool for treatment, payment, or health care operations purposes, provided that certain conditions are met. In accordance with the HIPAA Privacy Rule at 45 CFR, Subparts A and E, HIPAA requires an individual to authorize uses and disclosures of PHI, unless an exception applies. Per 45 CFR § 164.502, one such exception allows PHI to be used and disclosed for treatment, payment, and health care operations. A HIPAA covered entity may disclose PHI to service providers, known as business associates, for these purposes, provided that certain contractual requirements are in place and the business associate does not use or disclose PHI for its own purposes. However, given the ways in which generative AI tools process data and iteratively improve and learn, it is not always clear to covered entities whether PHI may be input into generative AI tools, even where the developer of the tool intends to serve as a business associate and has established safeguards to protect the confidentiality of PHI. As stated in the RFI:

> [I]n healthcare, regulations for medical devices, telehealth, and patient privacy were designed around human clinicians and discrete medical device updates. It may create challenges to apply the same policy framework for overseeing continuously updating AI diagnostic tools and ensuring explainable clinical recommendations.

Uncertainty about the permissibility of HIPAA-regulated entities using these tools, which are routinely leveraged in other sectors, could chill adoption and delay the health care industry's realization of their benefits. Thus, it would be helpful to clarify that where PHI is processed through a generative AI tool for treatment, payment or health care operations, only the minimum amount of PHI is processed for such purposes, and there is limited risk of the PHI being used or further disclosed for other purposes, given zero-day retention or similar controls, this qualifies as a permissible use and disclosure of PHI under HIPAA. Notably, this offers individuals additional protections in the treatment context, given that the current HIPAA rules do not require a health care provider's disclosure for treatment purposes to meet the minimum necessary standard.

Proposed guidance: HHS should issue an FAQ or other guidance clarifying the permissibility of these activities to avoid a situation where the lack of regulatory clarity and may delay AI adoption, increase compliance costs, and slow innovation.

D. Patient Rights

We recommend clarifying that an individual's rights with respect to their PHI are subject to a reasonableness standard. HIPAA provides individuals with multiple rights regarding their PHI, as specified at 45 CFR §§ 164.522–164.528, including rights to access, amend, or receive an accounting of disclosures of their PHI. When an individual exercises these rights, their requests may cover information dating back as many as six years. Upon receipt of an individual rights request, a HIPAA-regulated entity must timely review certain of its systems for responsive records, and action the request as appropriate.

The rules granting these rights were written decades ago, and did not contemplate the sophistication and complexity of modern AI technologies. It can be difficult and time-consuming for an organization to validate where data resides within such systems, and to produce the requested information or make requested changes. This challenge is compounded as organizations deploy AI systems that interconnect, such as multi-agent systems, and that process and share data in ways that can be difficult to track and document. Amending the rules to require reasonable efforts to respond to individual rights requests would recognize the practicalities organizations face when responding to these requests, while still honoring the individual rights set out under HIPAA.

Proposed guidance: HHS should issue guidance clarifying that a HIPAA-regulated entity's reasonable efforts to action an individual's request to exercise rights with respect to PHI processed by an AI system satisfy the entity's obligations under HIPAA. This can help avoid applications of HIPAA rules that hinder beneficial AI uses.

E. Transparency Requirements in HTI-1 for Decision Support Interventions (DSI)

AdvaMed urges ONC and OSTP to withdraw or substantially revise the current transparency provisions in the HTI-1 rule as applied to Decision Support Interventions (DSIs). While the stated goal of promoting explainability and clinician confidence in AI-enabled tools is well-intentioned, the resulting policy has proven misaligned with actual clinical and regulatory needs.

The HTI-1 transparency requirements impose uniform documentation and disclosure obligations across all DSIs, without consideration of risk or existing practices and requirements. The HTI-1 transparency requirements create an administrative burden without evidence that clinicians or patients find this information meaningful or actionable, particularly for lower-risk products and technologies. Additionally, transparency obligations should leverage existing authorities already available to the FDA, FTC, and other agencies to address safety or performance concerns. ONC and OSTP should focus their oversight on technologies that pose genuine risks, while relying on existing labeling, post-market surveillance, and quality-system requirements to ensure appropriate transparency for all others. FDA-regulated devices are subject to existing disclosure requirements. Additional disclosure requirements from ASTP/ONC could introduce redundancy and burden that would not support improved clinical decision making.

AdvaMed recommends that ONC and OSTP coordinate with FDA to develop a harmonized, risk-based framework that encourages meaningful, evidence-based transparency while avoiding unnecessary regulatory duplication.

IV. CONCLUSION

As the U.S. Government seeks to ensure that AI-enabled products across all industries are used safely, we appreciate the opportunity to provide feedback on regulatory priorities and recommendations that

impact medical technologies. AdvaMed member companies take seriously the trust patients place in them and have consistently acted to identify best practices that balance innovation with patient protections. Thank you for the opportunity to submit these comments. Please consider AdvaMed as a resource as you consider regulations related to AI and medical devices.

Thank you in advance for your consideration of AdvaMed's comments. Please do not hesitate to contact me with any questions by email at cwhite@advamed.org.

Sincerely,
/s/
Christopher L. White
General Counsel & Chief Policy Officer
Advanced Medical Technology Association (AdvaMed)