American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

February 23, 2026

Steven Posnack
Principal Deputy Assistant Secretary for Technology Policy
Department of Health and Human Services
Mary E. Switzer Building
330 C Street SW
Washington, DC 20201

Submitted Electronically

RE: RIN 0955-AA13 Request for Information: Accelerating the Adoption and Use of Artificial Intelligence as Part of Clinical Care

Dear Deputy Assistant Secretary Posnack,

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to provide comment on the Health and Human Services (HHS) request for information on accelerating the adoption and use of artificial intelligence (AI) as part of clinical care.

We applaud HHS for evaluating regulation, reimbursement, and research and development opportunities to advance the adoption of AI tools to support clinical care. Our member hospitals and health systems have seen AI tools' potential to improve outcomes, increase access and reduce costs. From ambient listening technologies assisting with clinical documentation to chatbots helping with scheduling and triaging to algorithms supporting clinician interpretation of images, AI-based tools have already made a significant positive impact on hospitals and the patients they serve.

Given AI's potential to drive efficiencies and enhance the quality of care, our members have urged that policy frameworks strike the appropriate balance of flexibility to enable innovation while ensuring patient safety. Attached you will find our recommendations to the three policy areas identified in the request for information (regulation, reimbursement, and research and development), as well as feedback on specific questions.

To accelerate AI adoption, we urge HHS to:

- **Synchronize and leverage existing policy frameworks to avoid redundancy.** While AI policies should be flexible to keep pace with innovation, they also should be synchronized and integrated with certain existing health care policy frameworks to minimize redundancies.
- **Remove regulatory barriers.** Certain statutes and regulations in the health care ecosystem, such as the patchwork of state privacy laws and 42 CFR Part 2, have indirectly impacted hospitals and health systems' ability to develop and deploy certain AI tools. We provide recommendations on ways to reduce regulatory barriers that inhibit the development and deployment of AI tools.
- **Ensure the safe and effective use of AI.** The AHA recommends policies that ensure clinicians are included in the decision loop for algorithms that may impact access to care or care delivery, provide consistency in privacy and security standards for third-party vendors and use post-deployment standards for health care AI to ensure ongoing integrity of tools.
- **Align incentives and address infrastructural factors.** Appropriate incentives and infrastructure investment are necessary to expand AI in health care. These are critical for both provider readiness and patient adoption. That being said, reimbursement for AI tools should not come at the expense of other medical services.

Our members recognize the potential of AI to transform care delivery and address some critical challenges the health care ecosystem faces, such as escalating costs, staff burnout and rising administrative burden. We look forward to partnering with HHS on policy approaches that can help AI realize its transformative potential. Our detailed comments are attached. Please contact me if you have questions, or feel free to have a member of your team contact Jennifer Holloman, AHA's director of health IT policy, at jholloman@aha.org.

Sincerely,

/s/

Ashley Thompson
Senior Vice President
Public Policy Analysis and Development

Attachment A: Accelerating AI Adoption Detailed Responses

Appendix A. Accelerating AI Adoption Detailed Responses

REGULATION

The AHA applauds the administration's recognition that excessive and overly restrictive regulations can increase costs, reduce access to care, stifle innovation and hamper competition.

The AHA has provided recommendations to the Office of Management and Budget, HHS, Federal Trade Commission and Department of Justice on ways to reduce the regulatory burden on hospitals and health systems.[1,2,3,4] We have also provided comments to the Office of Science Technology Policy on ways to reduce regulatory burden, specifically to support the advancement of AI tools in response to its request for information on regulatory reform for AI.[5] We appreciate that HHS continues to seek ways to reduce regulatory barriers to accelerate the adoption of AI in clinical care through this request for information.

We have recommendations for the regulatory framework to accelerate AI adoption for clinical care, including:

- Synchronizing policies with existing regulatory frameworks.
- Withdrawing certain proposals from the HIPAA security proposed rule.
- Strengthening federal HIPAA preemption.
- Removing the remaining 42 CFR Part 2 requirements.
- Including trained clinicians in the decision loop for health care AI tools that impact access.
- Applying the same privacy and security standards for third-party vendors as covered entities and business associates.
- Developing risk-based post-deployment standards for AI-enabled medical devices.
- Issuing clarifying guidance on clinical versus administrative applications.

Additional details follow.

Synchronize with Existing Regulatory Frameworks

In general, the AHA believes that AI policies should be flexible to keep pace with the rapid pace of innovation. At the same time, AI policy also should be synchronized and

---

[1] https://www.aha.org/lettercomment/2025-05-12-aha-response-omb-deregulation-rfi
[2] https://www.aha.org/lettercomment/2025-07-14-aha-comments-hhs-rfi-maha-initiative
[3] https://www.aha.org/lettercomment/2025-05-23-aha-comments-ftc-anticompetitive-deregulations-rfi
[4] https://www.aha.org/lettercomment/2025-05-23-aha-comments-doj-anticompetitive-deregulations-rfi
[5] https://www.aha.org/lettercomment/2025-10-27-aha-responds-ostp-request-ai-policies-health-care

integrated within certain existing health care policy frameworks to minimize redundancies. AI poses novel challenges from a policy development perspective, with many existing regulations for medical devices, patient privacy and payment designed around static technologies. Nevertheless, the AHA believes that AI policy should not be considered in a vacuum, as it intersects with a wide range of other critical policy areas with their own regulatory frameworks. Some areas of intersection include:

- **Data Privacy.** HIPAA provides baseline federal standards for the protection of personal health information. HIPAA covers a wide range of health information technology applications, including AI.
- **Cybersecurity.** The National Institute of Standards and Technology cybersecurity framework and the HHS cybersecurity performance goals provide reliable voluntary standards frameworks for cybersecurity.
- **Premarket Testing.** The Food and Drug Administration (FDA) regulations for Software as a Medical Device require testing of the safety and efficacy of AI-enabled medical devices through a premarket submission program.
- **Transparency.** The Assistant Secretary for Technology Policy/Office of the National Coordinator for Health IT (ASTP/ONC) requires certified health IT to meet certain transparency requirements for AI.
- **Anti-bias and Discrimination.** Any entity receiving federal financial assistance, including all health care providers and insurers, is prohibited from using AI tools and algorithms that discriminate through the HHS Office for Civil Rights (OCR) Anti-Bias and Discrimination regulations.
- **Access to Care.** The Centers for Medicare & Medicaid Services (CMS) Medicare Advantage regulations specify that AI cannot “act alone” to terminate or deny services. These regulations also establish that the health plan must ensure the tool is accurate and bias-free.

Certainly, there are important questions about how to update or clarify how existing regulations apply to AI tools, and where there may be gaps in regulation. However, establishing standalone AI regulation outside of these existing frameworks may unintentionally lead to redundancies and inefficiencies, as well as create confusion about which rules would apply in which circumstances. Ultimately, this would hamper innovation and impose artificial barriers on the development of AI tools. **For these reasons, we encourage HHS to synchronize policies with these existing regulatory frameworks.** We also encourage cross-agency coordination and guidance to ensure that policies are aligned.

Withdraw 2024 HIPAA Security Rule Proposals

Health data privacy and security are essential for patient safety and quality of care. This applies not only to AI tools, but also to any persons, entities or tools that leverage or exchange personal health information. HIPAA provides sound foundational standards for privacy, security and breach notification. While certain regulations have provided

clarifying guidance, other regulations would add unnecessary burden and run counter to HIPAA's original purpose of protecting health information.

For this reason, the AHA urges HHS to withdraw the Biden administration's proposed "HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information." This rule included several technically infeasible and misguided policies that would fail to strengthen protections for health information while penalizing hospitals for issues beyond their control. For example, the rule would require restoration of electronic information systems and data within 72 hours of a cybersecurity incident. This arbitrary timeframe would be infeasible in particularly complex cyberattacks. Furthermore, it may have the unintended consequence of increasing risk by requiring hospitals to bring systems online before they can complete a full threat assessment and isolate their exposure to further attacks. These rules also place the onus for ensuring cybersecurity on hospitals rather than the broader ecosystem. Given that most PHI data breaches reported to OCR were the result of hacking incidents targeting non-hospital health care providers, including third-party service and software providers, cybersecurity standards must address the full spectrum of stakeholders that collect, hold or transmit personal health information. The AHA does not support proposals for mandatory cybersecurity requirements levied on hospitals as if they were at fault for hackers' success in perpetrating a crime. Instead, the AHA supports voluntary consensus-based cybersecurity practices such as the HHS cybersecurity performance goals.

Strengthen Federal HIPAA Preemption

While HIPAA generally preempts contrary state law, there are specific exceptions to that preemption that have enabled a plethora of differing state laws that bear on health data privacy.

The current approach to preemption has burdened hospitals and health systems with a myriad of overlapping legal requirements, raising compliance costs and diverting limited resources that could otherwise be used on patient care. In addition, the patchwork of state and federal health information privacy requirements remains a significant barrier to the robust sharing of patient information necessary for coordinated clinical treatment. For instance, it makes it much more challenging for providers to use a common electronic health record that is a critical part of the infrastructure necessary for effectively coordinating patient care and maintaining population health. It also impedes the development and deployment of AI tools, as data drives algorithmic validity.

We encourage the administration to work with Congress to address this issue and enact a full HIPAA preemption provision. HIPAA is more than sufficient to protect patient privacy and, if interpreted correctly, it strikes the appropriate balance between health information privacy and valuable information sharing. Varying state laws only add costs and create complications for hospitals and health systems. As such, the

AHA reiterates its long-standing recommendation that Congress strengthen HIPAA preemption.

Remove Remaining 42 CFR Part 2 Requirements

We urge the administration to work with Congress to remove remaining requirements under 42 CFR Part 2 that hinder care team access to important health information. These regulations require separate maintenance of records on substance use disorder (SUD) information, which prevents the integration of behavioral and physical health care because the patient data cannot be used and disclosed like all other health care data. This can also affect SUD providers' ability to leverage AI tools for care delivery. Despite regulatory changes in recent years, the regulations in Part 2 are outdated, fail to protect patient privacy, and, in fact, erect barriers to providing coordinated, whole-person care to people with a history of SUD. By working with Congress, the administration can resolve the statutory conflicts that prevent full alignment of 42 CFR Part 2 requirements with the HIPAA requirements that govern other patient health information.

Include Trained Clinicians in Decision Loop for Health Care AI Tools That Impact Access

A key driver of excessive administrative costs for hospitals and health systems is the onerous requirements imposed by commercial insurers to check patients' eligibility for coverage, bill for payment, and process prior authorizations and coverage denial appeals. Most claims initially denied by insurers (70%) are ultimately paid, meaning a significant amount of administrative cost is a complete waste.[6]

To make matters worse, commercial insurers' use of AI to determine disposition of claims and prior authorizations has exacerbated inappropriate denials. A U.S. Senate Permanent Subcommittee on Investigations report from last year found that certain plans had significant increases in prior authorization denials, in part driven by automated tools, and that the use of AI for prior authorization potentially targeted financial gain over medical necessity.[7]

To mitigate this, we have advocated for HHS and congressional action to ensure that clinicians — not just AI tools — are included in the decision loop for any recommendations of partial or full denial of requested items or services.[8,9] While

---

[6] https://premierinc.com/newsroom/policy/80-premier-members-call-for-medicare-advantage-changes-to-address-payment-denials-and-delays
[7] https://www.hsgac.senate.gov/wp-content/uploads/2024.10.17-PSI-Majority-Staff-Report-on-Medicare-Advantage.pdf
[8] https://www.aha.org/lettercomment/2025-09-29-aha-supports-administration-facilitating-health-insurer-pledge-reform-prior-authorization
[9] https://www.aha.org/testimony/2025-10-09-aha-statement-record-senate-help-committee-hearing-ai-health-care

the use of AI tools to more quickly process prior authorizations is not inherently problematic, it is imperative that any recommendation to deny care, whether AI-generated or not, is independently reviewed by a clinician. Further, human reviewers should have the requisite training and expertise to provide an informed medical decision about a patient's condition and the proposed treatment plan.

We have also urged for algorithmic transparency so that clinicians can understand the reason a request was denied. Providers and patients are generally unaware when AI tools are used in the prior authorization process, much less have visibility on the inputs that drove a recommendation for approval or denial. Indeed, recent data from a survey of payers across 16 states conducted by the National Association of Insurance Commissioners show that only 23% of plans disclose to providers how and when AI is used.[10]

Apply the Same Privacy and Security Standards for Third-party Applications That Hold/Process PHI as Covered Entities and Business Associates

According to the HHS OCR, the number of individuals impacted by health care data breaches increased from 27 million in 2020 to a staggering 259 million in 2024.[11] Notably, most protected health information (PHI) data breaches reported to OCR were the result of hacking incidents targeting non-hospital health care providers, including third-party service and software providers.

AI systems rely on large data sets to maximize their predictive power. However, aggregating large data sets may also pose unique cybersecurity vulnerabilities that can further be exposed by privacy and security standards gaps. With the rise in third-party vendor PHI data breaches, it is essential that entities that hold or process PHI (including certain AI vendors that may not meet the definition for covered entities or business associates under the current law) and are not currently covered by HIPAA be subject to similarly rigorous privacy and security standards.

We recommend that third-party entities (including AI vendors) that collect, hold or transmit PHI should be held to the same standards and accountability as covered entities and business associates. Third parties also should be accountable for the privacy and security of data they pull from covered entities and business associates.

Develop Risk-based Post-deployment Standards for AI-enabled Medical Devices

Hospitals and health systems continually assess the strengths and limitations of all AI models they use. The "black box" nature of many AI systems can make it more

---

[10] https://content.naic.org/sites/default/files/inline-files/NAIC%20AI%20Health%20Survey%20Report%20.pdf
[11] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

challenging for hospitals and health systems to identify flaws in models that may affect the accuracy and validity of an AI tool's analyses and recommendations. There are many reports of certain AI tools producing "hallucinations" or false results based on flaws in model design or biases in underlying data. These factors underscore the importance of ongoing developer testing to maintain AI model validity.

As we recently commented to the FDA in response to its request for public comment, "Measuring and Evaluating Artificial Intelligence-enabled Medical Device Performance in the Real-World," we encourage agencies to pursue risk-based approaches to monitoring and evaluation activities, whereby factors for potential risk to quality and patient safety are accounted for in the measures and scope of monitoring.[12] In the spirit of a risk-based approach, the FDA could consider adding requirements for manufacturers to conduct a range of monitoring, from periodic revalidation activities to ongoing surveillance, depending on the risk level of the AI tool. In developing such frameworks, agencies should seek feedback from device makers, hospitals and other providers, as well as standards development groups.

At the same time, evaluation and monitoring activities should not be overly burdensome and resource-intensive. As the FDA considers approaches to AI measurement and evaluation, we encourage the agency to consider end-user burden and take steps to minimize it. A risk-based approach to measurement and evaluation could focus scarce resources, such as time, personnel and cost, on the highest-risk applications and also align with the approach of domestically accredited and international standards development groups.

Continue to Clarify Guidance for Clinical Versus Administrative AI Tools

Section 201(h) of the Food, Drug and Cosmetic Act identifies that certain AI applications are considered medical devices if they are "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease." The 21st Century Cures Act excluded certain AI tools from the purview of medical device oversight. For example, this statute excludes certain clinical decision support tools from the definition of "medical devices," so long as they *support* clinical decision making, with the clinician independently reviewing recommendations. Clinical decision support tools are often built to address a particular challenge for a specific period. Additional requirements can add barriers to delivering timely solutions and may also be impractical if the tool is only designed to support clinicians for a short timeframe (such as six months). We appreciate that the FDA has attempted to issue clarifying guidance on its interpretation of the statute. However, given the pace of technological advancement, we encourage HHS to continue issuing non-binding guidance that includes examples, use cases and frequently asked questions. Guidance on how federal frameworks apply to non-medical devices would be especially helpful, and could include considerations for

[12] https://www.aha.org/lettercomment/2025-12-01-aha-letter-fda-ai-enabled-medical-devices

documentation, monitoring, security obligations and reporting requirements. As a coordinating entity, HHS can provide unifying guidance across OCR, ASTP/ONC, CMS, FDA and research entities to support the safe use of non-medical AI tools.

REIMBURSEMENT

The AHA recognizes the pivotal role that AI plays in care delivery today and its potential to transform the patient and provider experience in the future. We applaud HHS for acknowledging the continued evolution of AI tools and the desire to consider updated methodologies to appropriately reimburse for these services. While hospitals and health systems recognize the potential benefits of AI solutions, inadequate reimbursement has left many without the resources to invest in the infrastructure necessary to develop and deploy AI tools. Implementing new technologies and standards often requires significant financial investment, education and workflow changes for health care providers. Ensuring appropriate reimbursement can support wider adoption of these tools and ultimately support improved access to services. Although there are some forms of reimbursement for AI for inpatient, outpatient and physician services (including new technology add-on payments and ambulatory and procedural codes), they are narrowly defined and do not account for the full spectrum of AI tools. Furthermore, they do not capture all cost factors associated with AI tools.

We have provided reimbursement recommendations to CMS through requests for information as part of our calendar year (CY) 2026 outpatient prospective payment system (OPPS) and CY 2026 physician fee schedule (PFS) comments.[13,14] We believe updates to payment for AI should not come at the expense of other services. We also have feedback on cost factors to consider to "right-size" payment for AI. Finally, aside from reimbursement, cross-agency coordination can support needed infrastructure investment, particularly to support AT advancement in rural and underserved areas. Additional details on reimbursement recommendations are detailed below.

Updates to AI Payment Should Not Come at the Expense of Other Services

In general, reimbursement for hospitals, hospital outpatient departments and physicians has fallen short. Despite escalating expenses, Medicare reimbursement continues to lag behind inflation — covering just 83 cents for every dollar spent by hospitals in 2023, resulting in over $100 billion in underpayments, according to an AHA analysis of our Annual Survey data.[15] As we recently noted to the Medicare Payment Advisory Commission, the Medicare program has not fully covered the costs of serving Medicare

---

[13] https://www.aha.org/lettercomment/2025-09-15-aha-comments-cms-cy-2026-outpatient-asc-proposed-payment-rule
[14] https://www.aha.org/lettercomment/2025-09-12-aha-comments-cms-cy-2026-physician-fee-schedule-proposed-rule
[15] https://www.aha.org/costsofcaring

patients since 2002 — *a full 23 years ago.*[16] The inadequacy of Medicare reimbursement can also be seen in physician reimbursement. Data from the American Medical Association indicate that physician payment has dropped by 33% since 2001, when accounting for inflation.[17]

The budget-neutral payment increases have meant that increases in certain services have resulted in cuts to others. **While we support "rightsizing" of payment for SaaS, this should not come at the expense of other services.**

Consider Other Cost Factors When Determining Payment for AI Tools

Implementing new technologies and standards often requires significant financial investment and workflow changes for health care providers. Expanded adoption of tools requires alignment of incentives. **While we appreciate the efforts to update reimbursement for new technologies, historical payment within OPPS and PFS structures has not fully accounted for the costs of these services.** This includes payment for certain CPT codes for AI, as well as bundled payment in risk-based arrangements.

There are specific factors that HHS should consider when setting payment rates for AI tools, since the costs associated with developing, deploying and maintaining AI tools extend beyond the software. Examples of cost factors that should be considered include:

- **Clinical Time for Validation.** AI-enabled tools augment — not replace — human capacity. In fact, these tools still require significant human direction, such as when developing treatment plans and supervising outcomes. For example, while an AI-enabled tool may recommend a particular course of treatment, ultimately a clinician is still making the final decision in consultation with patients and their caregivers. Reimbursement should account for the time required to validate AI outputs.
- **Maintenance.** AI and Software as a Service (SaaS) tools require stakeholders to engage in routine maintenance and post-deployment testing to ensure the ongoing integrity of tools. Maintenance may include technology vendors, developers and providers.
- **Cybersecurity Insurance.** While the expansion of SaaS offerings holds tremendous promise, there are also potential cybersecurity risks. According to U.S. government reporting, the most significant cyber threats targeting U.S. critical infrastructure, including health care, originate from noncooperative foreign

[16] https://www.aha.org/lettercomment/2026-01-09-aha-comments-medpac-payment-update-recommendations
[17] https://www.ama-assn.org/system/files/2025-medicare-updates-inflation-chart.pdf

jurisdictions.[18,19,20,21] Cross-border hacking incidents, which result in the theft of PHI and ransomware attacks targeting health care, have increased dramatically, rising nearly tenfold since 2020. As previously discussed, most PHI data breaches reported to OCR were the result of hacking incidents targeting non-hospital health care providers, including third-party service and software providers. The rise in frequency and severity of cyberattacks accompanying the expansion of SaaS tools has driven increased cybersecurity premiums. Reimbursement models should account for this. Just as malpractice is factored into payment (e.g., malpractice relative value units in the PFS), we encourage rising cybersecurity costs also be considered.

- **Software and Storage Fees.** These costs also include software licenses, as well as data storage. SaaS offerings generally rely on large data sets, which also require servers. We encourage CMS to consider the costs for maintaining this underlying data infrastructure.

Address Infrastructure Barriers

The expansion of digital health products, including AI tools, to rural and underserved populations has been hindered in part by a lack of access to enabling technologies (such as broadband, reliable Wi-Fi or smartphones) and education to support digital literacy. Infrastructure investment is needed to support AI tool advancement in these communities.

Indeed, the Federal Communications Commission (FCC) reported that in 2020, over 22% of Americans in rural areas lacked access to appropriate broadband (fixed terrestrial 25/3 Mbps) compared to 1.5% of urban areas.[22] Furthermore, according to a recent report from the Assistant Secretary for Planning and Evaluation, over 26% of Medicare beneficiaries reported not having computer or smartphone access at home.[23] The lack of infrastructure, such as broadband and reliable Wi-Fi, has contributed to the "digital divide," where rural and other underserved areas have less access to digital services, including AI tools for clinicians and patients. These data points suggest that investment in foundational infrastructure and educational resources may increase providers' and patients' access to digital health and AI applications**.** We recognize that some of these constraints do not fall exclusively under HHS' purview. Therefore, we encourage cross-agency collaboration to develop training and potential grant funding

---

[18] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf
[19] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[20] https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-on-ransomware-attacks-against-hospitals-and-other-healthcare-facilities-and-services/
[21] https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
[22] https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2020-broadband-deployment-report
[23] https://aspe.hhs.gov/sites/default/files/documents/4e1853c0b4885112b2994680a58af9ed/telehealth-hps-ib.pdf

opportunities to support patient educational efforts on digital health tools. This could include coordination across agencies such as HHS, the FCC, the Department of Commerce, the Department of Agriculture and the Department of Education.

RESEARCH AND DEVELOPMENT

Hospitals and health systems across the country recognize AI's potential to transform research. AI's ability to process large amounts of data holds promise in supporting targeted therapeutics and precision medicine. We have also heard from members how AI is supporting clinical trial recruitment by processing large amounts of data to quickly identify potentially eligible candidates.

We appreciate that the administration is seeking ways to build regulatory sandboxes and testbeds to support AI-enabled research, as was identified in the AI Action Plan.[24] As HHS works to identify research and policy priorities, we urge the agency to establish mechanisms for provider input. Effective AI policies cannot be developed without engagement from the providers responsible for the care of patients that they serve. And while clinical use of AI tools is largely in pilot phases, the expansion to routine care underscores the need for ongoing engagement and partnership.

SPECIFIC QUESTIONS

Novel Legal and Implementation Issues

While AI tools offer significant potential benefits, many providers are concerned about liability ambiguity, particularly when AI algorithms could result in inaccurate recommendations that lead to poor outcomes. Indeed, the lack of clarity surrounding liability is a significant barrier to provider adoption of AI tools. AI systems are often developed and deployed with inputs from a variety of stakeholders, where providers are just one of many sources. Also, certain algorithm elements may be treated by developers as proprietary, which makes it challenging for hospitals and other AI users to identify model flaws, discrepancies between training data and real-world applications, or any model drift over time.

While many of these issues may intersect with case law and state-level malpractice statutes, HHS can play a vital role in supporting reasonable standards for developer transparency and post-deployment monitoring. Some of these issues underscore the importance of policies like post-deployment standards to ensure the ongoing integrity of tools and transparency standards for health IT certification. As the agency continues to explore novel liability challenges, we urge HHS to provide formal mechanisms for provider input.

---

[24] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

Vendor Certification

The volume of new entrants entering the health care AI space has made it challenging for hospitals and health systems to keep track of AI applications that may generate value. While hospitals and health systems have dedicated internal resources to support governance processes and pre-contract vetting, some hospitals may not have resources available to support this on a broader scale. Streamlined voluntary certification, built on industry standards, may provide a pathway for vendors to demonstrate functionality and provide baseline assurance to providers that certain standards are met. This can support responsible and scalable adoption of AI tools.

Promising AI Applications and Examples of AI Falling Short

AI holds the potential to drastically change hospital operations and patient care delivery. Among other benefits, these innovations can improve workflow, enhance the overall patient experience by reducing wait times and ensure timely medical interventions.

A few notable examples of promising AI applications in hospitals include:

- **Imaging/Radiology.** AI is significantly enhancing the accuracy and efficiency of X-ray and MRI reviews in hospitals. AI can detect and alert clinicians to subtle changes in tissue images, which is crucial for early disease detection.
- **Ambient Listening Tools.** These tools automatically transcribe and organize clinical notes. This reduces the administrative burden on health care providers, allowing them to focus more on patient care. Ultimately, these tools can reduce provider documentation time, increase appointment capacity and improve staff satisfaction.
- **Scheduling.** AI-powered scheduling tools are enhancing the efficiency of procedures and internal clinical operations by optimizing appointment times, resource allocation and staff schedules.

One example where AI is falling short can be seen in commercial payers' use of AI tools for prior authorization. Commercial payers' prior authorization processes have historically been plagued by high denial and overturn rates on appeal. One study of Medicare Advantage plans found that over 80% of denied prior authorization requests that were appealed were successfully overturned.[25] The onerous administrative burden has contributed to clinician burnout and has driven up costs. Utilization of AI tools for prior authorizations by commercial payers has actually catalyzed inappropriate denials, resulting in more administrative burden for providers to appeal. A recent American Medical Association survey also found that 62% of doctors think that payer use of AI is

[25] https://www.kff.org/medicare/nearly-50-million-prior-authorization-requests-were-sent-to-medicare-advantage-insurers-in-2023/

increasing denials for medically necessary care.[26] This is one cautionary example of where expanded use of AI tools without proper oversight can negatively impact patients' access to services and contribute to waste in the system. That is why the AHA has urged that trained clinicians be in the decision loop for AI tools affecting access to care.

Governance

Hospitals and health systems have worked to adapt their governance processes for AI use to meet the pace of technology advancement. Hospitals and health systems often use multi-disciplinary teams to review AI use cases, technologies and value over time. According to the AHA's Health IT supplemental survey, 74% of hospitals have multiple teams responsible for evaluating predictive AI, including (but not limited to) senior leaders, department leaders and IT staff, with many having specific committees for machine learning and/or clinical decision support.[27] And while hospitals remain committed to ensuring AI tools are accurate, safe and effective, this should not rest solely on hospitals and health systems.

While hospitals and health systems continually assess the strengths and limitations of AI models they use, third-party vendors must be responsible for the ongoing integrity of the tools they sell. The "black box" nature of many AI systems can make it more challenging for hospitals and health systems to identify flaws in models that may affect the accuracy and validity of an AI tool's analyses and recommendations. As such, post-market measurement and evaluation standards should be developed for vendors. Standards should include performance metrics, evaluation thresholds and communication requirements for ongoing performance to end users.

Additionally, some hospitals (particularly rural, critical access and other safety net hospitals) may not have the staff or resources to support governance structures and ongoing measurement activities. As such, many of these health care providers have not deployed AI tools. Resource and infrastructure barriers can exacerbate the "digital divide" in certain geographies, where rural and other underserved areas have less access to digital services, including AI tools for clinicians and patients.

---

[26] https://www.ama-assn.org/practice-management/prior-authorization/how-ai-leading-more-prior-authorization-denials

[27] https://healthit.gov/data/data-briefs/hospital-trends-use-evaluation-and-governance-predictive-ai-2023-2024/#DB80_Appendix_Figure_A2