Accolade
PERSONALIZED HEALTHCARE

**Accolade Response to the NSF & OSTP Request for Information on the National AI R&D Strategic Plan Action Plan**

**Submitted to:** National Science Foundation (NSF) & Office of Science and Technology Policy (OSTP)
**Submitted by:** Accolade, Inc.
**Date:** March 14, 2025

## Introduction

Accolade appreciates the opportunity to provide input on the National AI R&D Strategic Plan Action Plan, particularly as it relates to healthcare applications of AI. Artificial intelligence is becoming increasingly integrated into clinical decision-making, patient engagement, and healthcare operations, offering transformative benefits. However, to fully realize AI's potential in healthcare, federal AI policy frameworks must be privacy-preserving, secure, transparent, and fair, while also supporting innovation.

As the federal government refines its AI strategy, we emphasize the importance of modernizing regulatory frameworks, enhancing data security, and strengthening interoperability standards to ensure AI systems are both effective and trustworthy. Below, we outline key areas where federal R&D investment and policy modernization can help drive responsible AI development in healthcare.

## 1. AI-Specific HIPAA Modernization

The Health Insurance Portability and Accountability Act (HIPAA) was developed in a pre-AI era and does not fully address the complexities introduced by modern AI-driven healthcare solutions. While HIPAA provides a strong foundation for protecting patient data, AI's ability to process, analyze, and learn from large-scale health information presents new challenges that must be addressed to safeguard privacy while supporting innovation.

To ensure that AI aligns with privacy and security principles, we recommend:

- **Explicit AI Regulations:** Establish clear guidelines on how Protected Health Information (PHI) can be used in AI models. These regulations should ensure that de-identified data remains truly anonymized, with safeguards to prevent re-identification risks in AI-generated insights.

- **AI Model Transparency:** Require AI systems involved in clinical recommendations, patient triage, or diagnostics to disclose their decision-making processes to both providers and patients. AI models should be interpretable and explainable to ensure that medical professionals and patients understand how conclusions are reached.

- **Bias & Fairness Audits:** Implement regular bias assessments of AI models to prevent systemic discrimination in healthcare recommendations. AI models must be rigorously tested for fairness to ensure that healthcare disparities are not exacerbated.

### 2. Federated or Zero-Knowledge Data Models

AI systems should be designed to prioritize data security and minimize privacy risks while still enabling innovation in healthcare. Traditional centralized data models create significant security vulnerabilities, increasing the risks of data breaches. Instead, the federal government should support the development and implementation of privacy-preserving AI models that allow for decentralized data processing.

We encourage federal investment in:

- **Federated Learning Approaches:** AI models should train on decentralized datasets rather than requiring all patient data to be aggregated in a single location. This approach enhances data security and privacy while still allowing AI to learn from diverse patient populations.

- **Zero-Knowledge Data Processing:** AI systems should process patient information without storing identifiable PHI whenever possible. By ensuring that AI models can operate with minimal exposure to sensitive data, we can significantly reduce the risks associated with data breaches and unauthorized access.

### 3. Real-Time Consent & Patient Data Ownership

As AI becomes a decision-making partner in healthcare, it is essential to provide patients with greater control over how their health data is used. Current consent mechanisms are often static and difficult to manage, leaving patients without a clear understanding of how their data is being used in AI-driven healthcare applications.

To empower patients and build trust in AI, we recommend:

- **Real-Time Digital Consent:** Develop a national standardized framework for digital patient consent, allowing individuals to grant, revoke, or modify access to their health data dynamically. This framework should be interoperable across healthcare platforms and easily accessible to patients.

- **AI Transparency in Patient Engagement:** Require healthcare providers and platforms to notify patients when AI is being used in their treatment or care decisions. Patients should have the option to opt in or opt out of AI-based recommendations, ensuring that they remain in control of their healthcare journey.

**4. Secure API Standards for AI Interoperability**

As AI-driven healthcare applications increasingly interact with Electronic Health Records (EHRs), telehealth platforms, and clinical decision support tools, strong interoperability and security standards must be in place to protect patient data and ensure seamless integration.

We propose federal investment in:

- **Strong Encryption & Audit Logs:** AI-driven healthcare platforms should be required to implement robust encryption standards to secure API communications. Additionally, transparent audit logs should be maintained to track data access, modifications, and transfers in real time.

- **Common Security Frameworks:** Establish a federal security standard for AI-driven health data exchange, ensuring that AI applications comply with rigorous privacy and security protocols before being integrated into clinical workflows.

**5. AI-Driven Fraud Detection & Security Enforcement**

AI can play a transformative role in detecting fraud, securing patient data, and enforcing compliance with healthcare regulations. However, AI security enforcement tools must be proactively implemented and monitored to ensure effectiveness.

To enhance healthcare security, we recommend:

- **Real-Time AI-Powered Compliance Monitoring:** AI should be leveraged to detect HIPAA violations, unauthorized data access, and unusual behavior patterns in real-time. By deploying machine learning-based monitoring systems, healthcare organizations can quickly identify and mitigate security threats.

- **Automated AI Risk Assessments:** Before AI-driven health tools go live, they should undergo automated vulnerability scans to identify potential weaknesses. These assessments should be required for all AI applications processing patient data, ensuring security risks are addressed before deployment.

**6. The Role of NIST in AI Governance**

The National Institute of Standards and Technology (NIST) has played a critical role in establishing AI risk management frameworks and guiding the development of secure, fair, and trustworthy AI systems. NIST’s expertise will be crucial in ensuring that AI-driven healthcare innovations adhere to strong safety and security standards while fostering continued U.S. leadership in AI governance.

To further strengthen NIST's role, we recommend:

- **Enhancing AI Measurement & Benchmarking Tools:** NIST should continue developing AI performance assessment methodologies to evaluate bias, accuracy, and security risks in AI healthcare applications.
- **Supporting AI Testing & Evaluation:** Expand AI assurance labs to assess real-world AI implementation in healthcare settings, ensuring models perform safely and effectively before deployment.
- **Developing Interoperability Standards:** NIST should establish federal standards for AI-driven health data exchange, ensuring seamless integration across EHRs, AI-driven diagnostics, and telemedicine platforms.

**Conclusion**

AI has the potential to revolutionize healthcare by enhancing clinical decision-making, patient engagement, and operational efficiency. However, to maximize its benefits while minimizing risks, AI governance frameworks must evolve to address privacy concerns, bias mitigation, and security challenges.

Accolade urges the NSF and OSTP to prioritize investments in privacy-preserving AI models, real-time patient consent mechanisms, and AI-driven security enforcement as part of the National AI R&D Strategic Plan. We look forward to continued engagement on these critical issues and welcome the opportunity to collaborate on shaping a responsible and innovation-friendly AI future in healthcare.

Respectfully submitted,

[redacted]

Ardie Sameti
Vice President, AI and Platform
Accolade, Inc.

*This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.*