STATEMENT OF CHARLES WORTHINGTON
CHIEF TECHNOLOGY OFFICER AND CHIEF ARTIFICIAL INTELLIGENCE OFFICER
OFFICE OF INFORMATION AND TECHNOLOGY
DEPARTMENT OF VETERANS AFFAIRS BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
U.S. HOUSE OF REPRESENTATIVES
DATA PRIVACY AND ARTIFICIAL INTELLIGENCE"

JANUARY 29, 2024

Good afternoon, Chairman Rosendale, Ranking Member Cherfilus-McCormick, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today about the Department of Veterans Affairs (VA) efforts in patient and data privacy, and Artificial Intelligence (AI). I am accompanied today by Mr. John Oswalt, Deputy Chief Information Officer of Freedom of information Act, Records and Assessment Compliance, Office of Information and Technology (OIT); Dr. Gil Alterovitz, Director, VA National Artificial Intelligence Institute and Chief AI Officer, Veterans Health Administration; and Ms. Stephania Griffin, Director, Information Access and Privacy Office, Veterans Health Administration (VHA).

VA is committed to protecting Veterans' data while responsibly harnessing the promise of AI to better serve Veterans. While AI can be a powerful tool, its use and application needs to have the proper controls, oversight, and security guided by VA's Zero Trust Cybersecurity Strategy; and Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of AI.

In order to run the largest integrated health care system in the nation and deliver a myriad of benefits to eligible veterans, VA has a complex data ecosystem with over 1,100 petabytes of sensitive information, and an extensive digital footprint spanning over 500,000 desktops across 2,000 locations. To protect this environment, VA's Cybersecurity Strategy was established to unify an enterprise-wide solution that protects the Department's data at-rest, in-use, and in-motion.

The Department leverages sound cybersecurity practices to protect the confidentiality, integrity, and availability of our information and information systems now and in the future. These practices include physical, technical, and administrative controls and enables cybersecurity professionals to monitor, detect, and respond to cyber threats. These protections constitute a strong defense-in-depth strategy comparable to those deployed in the commercial sector. Identity Management is key in this area. Federal departments and agencies should require least privilege access to data resources and tiered user permissions to enforce separation of duties to those resources that house data. This testimony provides an overview of all VA currently does to protect Veterans' data, as well as note what challenges we currently face and where resources can best be allocated.

Protecting Data at Risk

VA uses the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) to comprehensively manage and report on privacy and security risk throughout the IT system lifecycle (hardware and software components). This enforces independent privacy and security reviews that prevent conflict of interest when conducting privacy and security assessments and audits. The overall RMF does not involve vendors in the determination of system security risk nor in the performance of security audits. As part of RMF, VA deploys a comprehensive Assessment and Authorization (A&A) program that requires independent or third-party security assessors to perform assessment reviews, testing, and audits against vendor hardware and software components to ensure that security risk is identified and mitigated or remediated to an acceptable level prior to deployment. Within the A&A process, the Authorizing Officials use the security and privacy posture of a system to determine if the risk to organizational operations and assets are at an acceptable level, in accordance with VA risk management strategy.

VA risk management aligns with NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations. VA security control requirements deploy a diverse set of information technologies for VA systems within the Department's IT footprint to reduce the risk and impact of potential exploitations of specific technologies and to defend against common mode failures. Additionally, the Department is aligning the program to VA's Data Governance Council to provide strategic direction and visibility across the enterprise.

This balanced risk management approach deliberately provides VA the guardrails it needs when considering emerging technology tools that have a large potential to improve Veteran health care and benefits such as Artificial Intelligence (AI).

Artificial Intelligence

VA is committed to responsibly harnessing the promise of AI to better serve Veterans. VA is excited about the potential of emerging AI technologies and how those technologies can empower the Department's mission on delivering world-class, secure technology solutions that enable a seamless, unified, efficient Veteran experience. To that end, VA was one of the first five Federal agencies to publish an AI strategy. VA's AI Strategy, published in 2021, which articulates a clear vision to improve outcomes and experiences for Veterans by developing trustworthy AI capabilities. It is imperative that VA and other government agencies implement AI responsibly and securely. VA needs to be very intentional and strategic about its implementation to ensure these technologies do not perpetuate bias or introduce inaccuracies. VA's goal is to maximize the potential value of AI to improve Veteran health and benefit outcomes and comply with Executive Order 14110 and upcoming Office of Management and Budget (OMB) memorandum.

As you know, VA has one of the Nation's largest and most extensively curated collections of health and benefits data in the world, representing a great opportunity to use AI with the potential to unlock improved outcomes for Veterans. AI at VA is at a

transition point, where solutions that leverage AI will graduate from the lab into enterprise-grade systems. VA's current execution plan for AI has the following four main workstreams: governance; execution of several high priority use cases; AI workforce development; and AI infrastructure.

Overview of VA's Use of AI in Health Care Delivery

VA has embraced the power of AI to revolutionize health care delivery. The Department is strategically leveraging this tool to improve the health care experience for the Nation's Veterans by enhancing patient care, streamlining administrative processes, and improving health care outcomes. By integrating AI into various aspects of Veteran health care, such as decision support systems, predictive modeling, and personalized care plans, VA is enhancing diagnostic accuracy and efficiency. VA is actively using AI in the area of predictive analytics, which uses vast amounts of data to identify patterns and trends, including predicting risks of cancers[1] and adverse outcomes, allowing for early and personalized interventions, ultimately improving health outcomes for Veterans. AI tools such as these hold the promise of optimizing efficiency of VA's health care delivery, while improving the quality of care provided to our beneficiaries.

Benefits and Potential of AI in Veteran Health Care

VA is building a network of cross-disciplinary experts to capitalize on VA data and drive AI research, development, and practical AI implementation to improve Veterans' health and benefit services. With over 120,000 clinicians serving more than 9 million patients across 1,200 medical facilities, VA possesses an unparalleled wealth of health care data. These data, which include over 10 billion medical images and the world's largest genomic database tied to medical records, can be leveraged to propel the United States to the forefront of AI leadership. Furthermore, as the Nation's largest integrated health care system, VA is uniquely positioned to test and scale effective AI solutions.

Effective AI implementation can improve staffing, development of novel treatments, patient safety monitoring, and disease prediction. VA is focused on using AI to alleviate provider burnout by reducing administrative tasks such as data entry. VA is currently hosting an AI Tech Sprint to source tailored AI solutions to further reduce burnout. In addition to reducing burnout, VA is also dedicated to accurately identifying health care providers, improving provider directories' accuracy to over 90%,[2] and enhancing access to care and patient safety. VA is leveraging AI in clinical settings as another tool available for providers. One example of AI in clinical use is GI Genius, a U.S. Food and Drug Administration -authorized system that aids in detecting concerning

[1] The official OIT Compliance, Risk, and Remediation AI Use Case Inventory submitted to OMB shows 10 use cases related to cancer.

[2] Council for Affordable Quality Healthcare (CAQH). (2023). Improve provider data management and accuracy. Available at: https://www.caqh.org/solutions/provider-data.

polyps during colonoscopies, leading to a 50% reduction in missed colorectal polyps compared to standard procedures.[3]

Addressing Concerns and Ensuring Accountability in AI Utilization

The main risks associated with AI are data breaches, biased predictions in health care, and patient safety. However, the use of Trustworthy AI[4] can mitigate these risks and lead to increased adoption, decreased risks, improved competitiveness, and higher returns on investment for VA. To ensure the safe and responsible use of AI, VA has developed its own Trustworthy AI framework aligned to VA's mission. Adopted in July of 2023, VA's Trustworthy AI framework outlines six principles for all instances at the agency to ensure that they are Purposeful, Effective and Safe; Secure and Private; Fair and Equitable; Transparent and Explainable; and Accountable and Monitored.

Within the National Artificial Intelligence Institute AI Network, VHA currently has several pilot efforts in place to increase safety, transparency, and trust in AI. The AI Institutional Review Board (IRB) module incorporates Trustworthy AI principles into the existing IRB process to protect Veterans participating in AI research and enhance transparency and trust in AI. The AI Oversight Committee pilot is another mechanism to instill trust and empower medical center directors to establish processes and systems of governance that support compliance.

Collaborations and Partnerships for AI Advancement in Veteran Health Care

We practice a high-level of continuous collaboration, while building many strategic partnerships, all to advance the development of Trustworthy AI innovations for Veterans, their survivors and caregivers, and American citizens, fostering a global impact. Our collaborations span multiple sectors—including other VA entities, Federal organizations,[5] academia, the military, international bodies, and private industry—enabling us to identify AI use cases; advance research and development capabilities; expand our reach to diverse populations and demographics; connect with top data science talent; and disseminate Trustworthy AI solutions. AI Tech Sprints are a prime example of how VA fosters connection with innovators outside of government to develop new solutions and improve Veteran care and experience. VA will complete two in this calendar year. [6] The current AI Tech Sprint focuses on reducing provider burnout and administrative burden, ultimately improving care for Veterans. Teams from across

---

[3] Wallace MB, Sharma P, Bhandari P, East J, Antonelli G, Lorenzetti R, Vieth M, Speranza I, Spadaccini M, Desai M, Lukens FJ, Babameto G, Batista D, Singh D, Palmer W, Ramirez F, Palmer R, Lunsford T, Ruff K, Bird-Liebermann E, Ciofoaia V, Arndtz S, Cangemi D, Puddick K, Derfus G, Johal AS, Barawi M, Longo L, Moro L, Repici A, Hassan C. (2022, July). Impact of Artificial Intelligence on Miss Rate of Colorectal Neoplasia. Gastroenterology. 163(1):295-304.e5. doi: 10.1053/j.gastro.2022.03.007.

[4] This framework helps organizations develop ethical safeguards across seven key dimensions of AI governance and compliance, ensuring the network remains: Private; Transparent and Explainable; Fair and Impartial; Responsible; Accountable; Robust and Reliable; and Safe and Secure.

[5] Current collaborators in the federal sector include the Office of the National Coordinator for Health Information technology; the Departments of Health and Human Services, Defense, and Energy; the FDA; the Defense Health Agency; the Center for Medicare and Medicaid Services; the National Institute of Health; and others.

[6] As required by EO 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (October 20, 2023). Available at https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf.

the Nation are competing to develop AI solutions in two distinct tracks that will support health care workers. Track one will focus on AI powered, advanced health care record integration, while track two will identify an AI solution to enable ambient dictation for clinical encounters to improve provider-Veteran patient connection and reduce clinicians' documentation burden. Additionally, utilizing Cooperative Research and Development Agreements provides us with the flexibility to transfer commercially useful technologies to the non-Federal sector.

Ethical Considerations in AI-Powered Decision-Making

With the vast potential of AI, VA is equally concerned about the ethical and effective use of AI. Governance plays a key role in building in proper checks and balances and guidance on how AI is ultimately put to work—ensuring AI initiatives conform with wider accepted practices. AI has risks and challenges, so VA is focusing on an AI strategy, ethical guidelines, and best practices across VA and with external partners to deploy trustworthy, secure AI, that benefits our delivery of health care and benefits to the Veteran community.

Currently, VA is piloting VA AI Oversight Subcommittees, created an AI Working Group, and created an AI IRB Pilot, which allows comprehensive vetting of AI use cases to determine if an AI model follows the principles of trustworthy AI per EO 13960 and other Federal regulations that protect human subjects. Finally, VA recognizes the importance and need for AI transparency and publishes AI use cases on our VA AI Inventory website, sharing VA's inventory with other government agencies and the public.

Conclusion

VA's patient and data security solutions must consider the interaction with users, the value to the Veteran, as well as the confidentiality, integrity, and availability of VA's information resources. With a balanced, risk-managed approach toward secure computing, we will maintain the confidence and trust of Veterans, our stakeholders, and the public. With the strategies, policies, and programs in place, the Department continues in its mission to protect and secure the information of, and services for, the Veterans. Mr. Chairman, Ranking Member and Members of the Subcommittee, thank you for the opportunity to testify before the Subcommittee today to discuss one of VA's top priorities. I am happy to respond to any questions that you have.