Good morning, my name is Nicholas Culbertson and I'm the CEO of Protenus. I bring testimony today to the Committee on Veterans' Affairs Subcommittee on Technology Modernization with three different perspectives: that of a former non-commissioned officer of the US Army, that of a patient treated by Veteran Affairs, and that of a former medical student turned CEO of a healthcare compliance analytics and health data privacy firm called Protenus.

In these roles, particularly in my current one, I have learned that health data privacy and security requirements are in constant juxtaposition of the need for health data sharing, interoperability, and innovation. On one hand, we need to make health data accessible to help improve direct patient care delivery speed and effectiveness as well as spur novel innovations, further accelerating the quality and capabilities of our healthcare industry. On the other hand, the more accessible health data becomes, the larger the threat surface becomes, exposing health data to privacy and security breaches, as well as misuse of data and fraud.

The tension between protecting health data and sharing health data is not something that should be addressed lightly. We need to share data and we need to protect it. Any standard that tips favor in one direction will either stifle innovation or compromise the integrity of arguably one of the most valuable types of data in the world. I want to thank the Subcommittee for its efforts to consider setting a higher standard for health data privacy while modernizing VAs electronic health record system and hearing my testimony on the topic.

In 2009, I prepped for my last deployment to Afghanistan with the 20th Special Forces Group where I served as a Special Operations Medic and Advanced Tactical Practitioner. As an SF Medic on pre-deployment, I was trained to use a tactical palm-pilot device and laptop system, known as the MC-4, that was intended to capture SOAP notes and other medical documentation on the battlefield. The intent of this program was that medical documentation could be electronically transferred to flight medics during a rushed MEDEVAC and that documentation would persist in the soldier's medical record all the way from theatre to VA. I was disappointed to learn, however, that despite the time we spent on training, this program did not work and the notes I drafted never left the expensive device I carried in theatre. Instead, I had to re-draft documentation that was filed manually and, hopefully, not lost during a soldier's trip through recovery.

As a veteran, I experienced the challenges associated with health data lost due to a lack of interoperability between the DoD and VA. After I left the military, I sought physical therapy from VA to continue treatment on my wrist that I fractured on my last deployment. Despite being certain of my broken wrist diagnosis, having seen the Xrays of the fracture myself, my VA physician told me that my wrist was never broken because there was no documentation for it and no copy of the Xray image in my file. As a result, I had to seek physical therapy through private insurance.

As a civilian, I have seen how the digitization of medical records has greatly accelerated patient care and innovation. While in medical school at Johns Hopkins University, I was fortunate to be able to participate in research using electronic medical records during Hopkins transition from

multiple electronic health record systems to one central system that currently spans the entire enterprise. While this upgrade made it easier to share health information, the magnitude of sharing is quite expansive. Not only do immediate care team members have access to a patient's record, but also any workforce member across the enterprise can now access any patient's record. Partner, affiliate, other business associates can also access patient data through health exchanges or other data-sharing programs. Both this increase in exposure and Hopkins's goal of being an innovation hub for health data allowed the opportunity to launch the startup that I now run.

At Protenus, we've developed artificial intelligence that proactively audits how every end-user accesses and uses electronic health information to ensure health systems are compliant with regulations designed to protect patient privacy. With our technology, we've seen first-hand how access to health data can be abused, causing harm to the health system and patients alike. And we've also seen how access to health data, when governed correctly, can spur amazing innovations that ultimately help improve patient care overall.

I've seen, first-hand, the limitations and risks associated with antiquated health technology systems. I've also seen how using technology in healthcare can create a slew of privacy and security challenges. So, privacy or innovation? The answer is both. We must find a way to promote innovation through accessibility and sharing. But we also must ensure that we do everything we can to protect health data from falling into the wrong hands. This is especially true of our veterans who deserve the best we can offer. The best we can offer combines both innovation and privacy.

This is an opportunity for VA to set a higher standard. As technology continues to improve and create better access, so too must our standards for security and privacy continue to meet that standard, as well.