OPTUM Serve™

Cybersecurity – protecting health information for millions of Americans every day

OptumServe™ is committed to helping federal agencies implement strong cybersecurity and data protection practices designed to protect the confidentiality and integrity of information systems and assets.

Federal agencies serve diverse and expansive populations and the need for world-class data security has never been greater. From military service members and veterans to state and local government populations, we have extensive experience deploying leading security solutions to help our clients stay ahead of evolving cybersecurity threats and risks to their data.

Market-leading approach for information security

Our information security approach includes integrated cyber defense capabilities that are constantly evolving to respond to new threats. Our cross-industry collaborations put us in a unique position to provide security for federal agency data and information. Optum®, and our parent company UnitedHealth Group, are the first companies in the health care industry to partner with the Department of Homeland Security's Enhanced Cybersecurity Services program, allowing Optum to provide additional levels of protection for our customers and gain direct intelligence briefings from the DHS.

Our cyber defense systems

Optum has more than 500 dedicated information security experts — some of whom hold government security clearances including DoD 8570, DoD 8140 — we have a market-leading approach to information protection that includes:

- **Security operations center** with integrated intelligence from federal and state agencies, as well as domestic and international industry partners
- **Vulnerability management** including penetration tests that determine the effectiveness of our information security program and defense capabilities through simulated attacks

OptumServe is part of Optum and the UnitedHealth Group family of companies. We provide health services and proven expertise to help federal agencies tackle some of the biggest challenges in health care. We partner with the Departments of Defense, Health and Human Services, Veterans Affairs and other organizations to modernize the U.S. health system and improve the health and well-being of the people they serve.

- **Security intelligence relationships** with government agencies and external cyberintelligence communities (FS-ISAC and HITRUST CTX)
- **Big data security** including enhanced data collection and event correlation capabilities analytics and insight
- **24/7/365 command center** that includes cyber forensic and security incident response capabilities that are frequently tested and hardened

Our experts review more than 10 petabytes of customer and internal data to identify patterns and trends over time that help us defend against cyberattacks, 24/7.

We proactively seek out vulnerabilities in the system by simulating cyberattacks, which yields insights that strengthen our security and improve threat recognition and response.

Our Tier 3 data centers are TIA 942-compliant, host more than 40,000 servers and provide more than 32 petabytes of primary storage. They support more than 4,000 applications and maintain business processes for more than 700,000 contracted health care providers and over 5,000 contracted health care facilities. We own and operate these data centers and hosting processes with a security-first mindset.

Security standards and frameworks

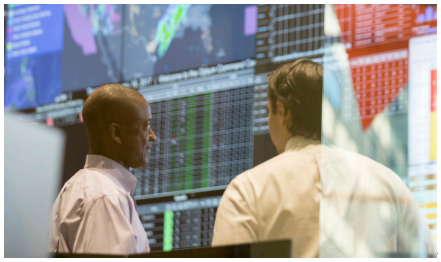
Optum has implemented policies and procedures based on best practices, risk assessment and legislative and contractual requirements for privacy and security set by the Federal Information Security Management Act of 2002 (FISMA), Federal Risk and Authorization Management Program (FedRAMP), HHS-OCIO Policy for Information Systems Security and Privacy, the Centers for Medicare and Medicaid Services (CMS) information security policies, other federal and state laws and other federal agencies. We also maintain NIST SP 800-53 and ISO9001-215-certified environments.

We are an authorized provider of a dedicated Amazon Cloud that is designed to host sensitive data, regulated workloads, and address the most stringent U.S. government security and compliance requirements. The AWS GovCloud (US)* is available to vetted government customers and organizations in government-regulated industries that meet AWS GovCloud (US) requirements.

Protecting data for federal agencies

Optum has been awarded a FISMA "Authority to Operate" (ATO) for several large systems that we manage at multiple federal agencies, some of which require FISMA high security.

In addition to those certifications and accreditations, our cybersecurity experts are proud to protect the information assets of millions of Americans every day. As a Fortune 5 company and one of the largest health care organizations in the world, we embrace the challenge of protecting the confidentiality, availability and integrity of our information systems and our clients' most important asset – their data. It is our priority 24/7.



We proactively seek out vulnerabilities in the system by simulating cyberattacks.

Our managed services infrastructure is HITRUST certified. We use a leading industry framework to guide and benchmark our cyber defense program. The framework is based on cyber defense practices used in the U.S. defense industry.

For more information, visit **optumserve.com** or call **1-800-765-6092.**

OPTUM Serve™ **optumserve.com**