Understanding the weak points in HHS cybersecurity

Five things you can do to start improving your agency's cybersecurity posture

Anyone involved in state government health and human services (HHS) understands the sensitive nature of the information stored within Medicaid benefit management systems. Breaches to these systems can expose the personal information of hundreds of thousands of residents, which can lead to identity theft, financial fraud, and a loss of public trust in government agencies. Ransoms in the tens of millions of dollars can be demanded to prevent the release or modification of stolen user data.

Unfortunately, the threat of cyberattacks is only growing. Readily available open-source and artificial intelligence (AI)-powered tools can now turn almost anyone into a sophisticated attacker. At the same time, the vulnerabilities they have to exploit are expanding. A little over a decade ago, many US states began to modernize and integrate their multiple HHS systems to provide a unified experience. The flexible, modular nature of a cloud-native architecture enabled agencies to more easily connect one application or network environment to another. The flip side of such flexibility and connectivity, however, is cybersecurity and compliance complexity, and a greatly expanded attack surface.

Why modern government is important

Government agencies in the US must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

How to respond

Effective security requires a comprehensive, multilayered approach across all HHS programs. While new technology is usually required, it's rarely the technology that's the complicated part, even in government environments, with their tangled web of aging legacy systems and cloud-based solutions. It's almost always the organization that's the real challenge—the "business" side.

Where to begin? Here are five things you can do to start improving your agency's cybersecurity posture:

1 Understand that security isn't about compliance

First is to break free of the idea that compliance and security are the same thing.

We see many agencies approach security as a "check-the-box-done" compliance exercise. The end goal isn't better security—it's simply to demonstrate compliance with a security or privacy standard such as NIST 800-53 or HIPAA.

But security is not a compliance exercise. It's a constantly moving target that requires constant attention. A system can be compliant and still not be secure. HIPAA compliance, for example, requires only that potential vulnerabilities be documented and a plan developed to address them—but not that the vulnerabilities actually be addressed in a specific time based on the criticality or potential impact.

2 Abandon a perimeter-based security mentality

Although they have migrated to a cloud-native architecture, many agencies still retain a perimeter-based security mentality.

In years past, the network perimeter provided nearly all the security that was required, with a limited number of entry points that could easily be monitored and controlled. But in today's highly decentralized and interconnected computing world, there is no network perimeter.

Security today requires a new approach, moving defenses from network-based perimeters to focus on users, assets, and resources. Zero-trust security is the leading such approach. It isn't a technology or compliance effort. It's a framework that requires an organizational transformation—a cultural shift in how organizations approach trust, access, and security at every level.

3 Make a commitment to security

Such cultural shifts are fast becoming existential necessities and, therefore, must become business priorities.

It's already happening in the private sector.

Satya Nadella, the CEO of Microsoft, for example, has traditionally focused on revenue growth as most CEOs do. But recently he decreed that everything must be secured by design. "We are doubling down on this very important work, putting security above all else—before all other features and investments."[1]

[1] Todd Bishop, "Haunted by breaches, Microsoft is 'putting security above all else,' vows CEO Satya Nadella," GeekWire, April 25, 2024

4 Focus on people more than technology

In many security incidents, people prove to be the weakest link. Increased training and organizational change management efforts often provide the biggest bang for the buck. Zero trust, for example, requires significant organizational change management as it substantially changes the way humans conduct their day-to-day duties and how agencies conduct their business.

5 Understand the trade-offs

Agencies seeking to address security vulnerabilities will quickly find themselves caught in a delicate balancing act, carefully trying to manage the competing priorities of compliance, security, and user experience.

It's difficult to overstate the importance of a seamless, easy-to-use, intuitive user experience. Such experiences are now demanded by users today and they're essential for agencies to effectively fulfill their mission. More intuitive and streamlined user interfaces can help to improve productivity and employee satisfaction. Real-time insights and data-driven decision-making can empower users and improve agency performance and client outcomes.

Yet simplifying access can introduce security vulnerabilities and opportunities for fraud, while overly complex verification processes may discourage or even prevent constituents—especially those with limited digital literacy—from seeking aid. Failure to comply with relevant standards can result in financial penalties, loss of funding, and erosion of public trust. However, prioritizing compliance can distract from efforts aimed at improving security.

You must strike a delicate balance between these competing priorities, proactively addressing challenges to ensure not only the safety and privacy of sensitive data but also the equitable and efficient delivery of essential services to those who need them the most. A risk-based approach to security will help you see the bigger picture and understand the implications of each decision to help you strike that balance.

Do what you can

There's no such thing as a perfectly secure system or environment—at least not one where people must be given access. But the convergence of growing cyber threats, regulatory complexity, and user expectations means HHS agencies must modernize their approach. It's essential to push as far as your resources will allow. Go after the low-hanging fruit. Attackers usually go after the systems that are the least secure.

How KPMG can help

KPMG LLP (KPMG) has worked with federal, state, and local governments for more than a century. We have over 1,500 dedicated cybersecurity professionals worldwide, and have been recognized by Forrester, IDC, and ALM Intelligence as a leading global organization of professional services for cybersecurity.[2,3,4]

We offer clarity and insight. As a trusted advisor, we can help you make sense of everything going on in the highly dynamic world of cybersecurity that can impact your mission, from regulatory mandates to emerging technologies. We can help align your efforts with leading practices from both the private and public sectors, and help keep you moving forward quickly with confidence and conviction.

We can help you from strategy through implementation. We're a multidisciplinary organization with business, technology, data and AI, risk, audit, and change management professionals working together as one team. We combine our cybersecurity acumen, government operations experience, cross-sector and cross-disciplinary skills, and alliances with leading technology providers to deliver robust security solutions that meet the needs of today's government organizations.

[2] ALM Intelligence Pacesetter Research, April 2022
[3] Philip D. Harris, "IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment," October 2023
[4] "The Forrester Wave, Quantification, Q3, 2023," Forrester, 2023

Contact us

Amiran Gelashvili
Managing Director, Advisory
Health and Government Solutions
KPMG LLP
816-256-1137
agelashvili@kpmg.com

Rahul Kohli
Principal, Advisory
Cyber & Tech Risk Lead for KPMG SLED Practice
KPMG LLP
781-812-9426
rahulkohli@kpmg.com

---

read.kpmg.us/modgov