Case Study: CMS
Overview

Industry
Government

Company Profile
The Centers for Medicare and Medicaid Services is a federal agency within the United States Department of Health and Human Services. It administers the Medicare program and works with state governments to administer Medicaid, the Children's Health Insurance Program (CHIP), and health insurance portability standards. CMS oversees Healthcare.gov, as well as quality standards relating to the Health Insurance Portability and Accountability Act (HIPAA), long-term care facilities, and clinical laboratories.

Business Situation
In 2015, the Centers for Medicare and Medicaid Services (CMS) collaborated with the U.S. Digital Service (USDS) to build the Quality Payments Program (QPP) interface, centered around shifting U.S. healthcare to a value-based payment model and away from traditional fee-for-service.

QPP replaced three government programs, each with its own identity management system. Login and account creation were significant hurdles, but the team faced another challenge: Designing an information-gathering process that would make sure the best providers received the greatest benefits. The team took an API-first approach, connecting to clinical data registries that already collect information about healthcare quality and outcomes.

Solution
CMS chose Okta to manage identity and access because of its industry leadership and its well-documented API. Okta API Access Management allows CMS developers to focus on streamlining the provider experience, while Okta securely controls access to the QPP website and API. Going forward, Okta will help modernize CMS backend systems to make its infrastructure more agile.

Benefits
- 58.4 million Americans on Medicare
- $702 billion in Medicare payments in 2017
- 15% of Medicare claims now submitted via the Okta-enabled API
- One website and API to gather information about healthcare quality and outcomes
- A modern identity infrastructure, with improved security, reliability, and scalability
- A streamlined user experience, delivered on time and within budget
CMS’s Journey

New government policies require new digital tools

In 2015, Centers for Medicare and Medicaid Services (CMS) collaborates with the U.S. Digital Service (USDS) to build the Quality Payment Program (QPP) interface, centered around shifting U.S. healthcare to a value-based payment model and away from traditional fee-for-service.

Sticky identity challenges

QPP replaces three government programs, each with its own legacy identity management system, which were mostly built in-house. Login and account creation are significant hurdles, but the team faces another challenge: Designing an information-gathering process that ensures the best providers receive the greatest benefits.

Connecting layers of access, securely

The team takes an API-first approach, connecting to clinical data registries that already collect information about healthcare quality and outcomes. CMS chose Okta to manage identity and access because of its industry leadership and its well-documented APIs.

A leap forward for government tech

Okta API Access Management allows CMS to focus on streamlining the provider experience, while Okta securely controls access to the QPP website and API. CMS developers declare the new API “a quantum leap forward.”

An API with monumental impact

The new QPP program delivers on time and on budget—a rare feat in government IT—and is instrumental in transforming the U.S. healthcare system. Going forward, Okta will help modernize CMS backend systems to make its infrastructure more agile.

58.4 million
Americans on Medicare

$702 billion
Medicare payments in 2017

15%
Medicare claims now submitted via the Okta-enabled API

Watch the video
okta.com/customers

Okta was able to log people in and out easily. It was nice to have one less thing to worry about.

— David Koh
Engineer, USDS
Story

New government policies require new digital tools

In 2015, the U.S. Congress passed the Medicare Access and CHIP Reauthorization Act (MACRA), mandating a transformative shift to a value-based healthcare payment model and away from traditional fee-for-service provider payments. The object was to incentivize and support doctors who demonstrably deliver quality care, so as to improve the quality of U.S. healthcare in general.

To support that shift, the Centers for Medicare and Medicaid Services (CMS) needed to build an online tool that healthcare providers could use to submit information about their services. Using that information, CMS would provide payment adjustments to providers based on the quality and outcomes of care.

CMS already had success collaborating with the U.S. Digital Service (USDS), a federal technology startup at The White House born in 2014 when President Barack Obama put out a call for tech industry experts to come to the aid of Healthcare.gov. That website’s technical problems threatened to derail the Affordable Care Act (ACA), which fell under the auspices of CMS. Since then, USDS technologists and UX designers had worked with CMS to modernize Healthcare.gov and make sure annual insurance enrollment periods progressed smoothly.

“We’re a team of technologists and designers and healthcare policy experts who truly believe that the future of healthcare should be focused on empowering doctors and patients,” says Crystal Yan, product and UX consultant at USDS.

At the root of sticky bureaucracy: Sticky identity challenges

The new MACRA tool, dubbed the Quality Payment Program (QPP), was a chance for CMS and USDS developers to build something from scratch using the modern IT principles they’d been working with since 2013. “What if we started at the beginning?” says David Koh, USDS engineer. “Could we do something that was transformative, that could bring modern technology into government in a way that had never been done before?”

QPP replaced three other government programs, each with its own website and legacy identity management system—built mostly in-house on old technology, using cumbersome processes. Providers had to create accounts in three different systems and keep track of those logins and passwords. The complicated account creation process created huge barriers.

“We wanted it to be easy for people to create an account,” says Koh. “We also wanted people to be able to use the accounts they had already created.”

Security and identity management were not a core strength for CMS developers—healthcare management was. The USDS team recommended they identify an identity management partner who could unify all three websites and bring the latest identity technology and skills to the QPP project.

Privacy was also paramount. When considering a new identity and access management solution, the team wanted it to integrate seamlessly with their new, modern technology stack, but it also needed to be completely secure. Two-factor authentication was essential to ensuring that sensitive, HIPAA-regulated patient information would be protected.

Reliability was also critical. “QPP is a little like doing your taxes,” says Koh. “There’s a window when doctors can apply for the whole year, and the payments they receive are based on what they submit. If the system goes down in the last week or the last day of that window, things get chaotic.”
Identity was one of the biggest hurdles we had to cross, but we also wanted to provide a good experience to QPP users. Okta helped us achieve both those goals.

— David Koh
Engineer, USDS
“94% of federal IT projects don’t deliver on time, or they’re over budget, or both. We wanted to be in that six percent, on time and under budget, and we succeeded.”

David Koh
Engineer, USDS

Connecting layers of access, securely

The API approach added another layer to the identity challenge. All of those data registry partners would need to connect to the QPP API seamlessly and securely. The team began looking at Okta, as the leader in the identity space, to serve as the data gatekeeper for partners, providers, and CMS employees.

“Okta had an easy-to-work-with API that we could plug into,” says Koh. Developer documentation for Okta APIs is a particular strong point, he says. “It’s made our lives much easier and allowed us to develop a much better product.”

Okta APIs fit with the modern infrastructure that CMS was building, as well. Okta offers HIPAA-compliant infrastructure, a requirement to meet the scale, reliability, and regulatory requirements of a large public-sector organization.

“We could see that it would eventually make a good enterprise solution for CMS,” says Koh. CMS administers hundreds of programs, in addition to QPP. With an Okta choice, the team would be setting a standard for how CMS would manage identity across its programs as it moved into the future.

Okta also offered its easy-to-use Multi-Factor Authentication product. “It was similar to what many of our users would have been used to on other services, like their email or their bank,” says Koh. The extra layer of protection would be critical for meeting HIPAA standards and protecting patient information.

Finally, the team was impressed with Okta’s administrator console and different administrator roles. When users called in with login issues, Okta allowed help desk admins to easily access just the right level of detail on user accounts. “Okta was able to give a good experience to that person at the service desk, so that they could give a good experience to our end user,” says Koh.

“One less thing to worry about.”

Today, QPP operates from a website that unifies the three original programs into a single experience. “The login experience was one of the first things we rolled out for QPP,” says Koh. “It had been such a big pain point for users in the past.”

Okta API Access Management allows CMS developers to focus on creating a streamlined QPP experience while Okta controls access to the website and API. While the team had to debug a few issues with the QPP system, having to do with how information gets imported or with service desk processes, “we didn’t have issues with Okta itself,” says Koh. “Okta was able to log people in and out easily. It was nice to have one less thing to worry about.”

The Okta Identity Cloud allows CMS to transform the user experience for healthcare providers, with a cloud-based architecture that easily accommodates millions of users, scaling up automatically during peak periods. In 2017, Okta received Moderate certification in the Federal Risk and Authorization Management Program (FedRAMP), further proving its commitment to keeping public-sector systems safe and secure.

Going forward, Okta will help modernize CMS’ backend systems and make its infrastructure more agile as the agency’s constituents continue to increase in number and frequency of authentications.
Okta had an easy-to-work-with API that we could plug into. It's made our lives much easier, and allowed us to develop a much better product.

– David Koh
Engineer, USDS
About Okta

Okta is the leading identity standard for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world’s largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,500 apps, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 21st Century Fox, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions more quickly by making it safe and easy to use the technologies they need to do their most significant work.

To learn more about Okta, visit:
http://www.okta.com

Subscribe to Okta’s blog:
http://www.okta.com/blog

Follow Okta on Twitter:
www.twitter.com/okta