# U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)

NEXTGEN EXTERNAL USER MANAGEMENT SYSTEM (XMS)

SEPTEMBER 7, 2022

# HHS HSPD-12 Program Overview

**1**

**HHS's Ecosystem is complex …**

… and spread across diverse mission areas. It is critical to secure access to HHS's digital resources and connect organizational and non-organizational users to its services to meet their mission objectives.

**2**

**HHS's HSPD-12 Program Provides Enterprise ICAM Services, including…**

… Credential Management, Logical Access Management, Physical Access Management, and Directory and Data services.

**3**

**Logical Access Management function focuses on …**

… digital identity lifecycle management and logical access throughout HHS and provides (among other capabilities) simplified sign-on to multiple applications for streamlined access.

# Secure Digital Experience for External Users – A Priority for HHS

A strong need for a more streamlined, secure and consistent user experience for external users resulted in the establishment of the NextGen External User Management System (XMS) program.

## The Need and the Opportunity

1. Multiple digital identities across HHS ecosystems complicate external end user experience
2. Secure, compliant and standards-based access for non-HHS external users
3. Consistent and secure experience using trusted identity and federated authentication

## Design Considerations

1. How can we provide a streamlined experience on a digital platform?
2. How can our solution provide coverage inclusive of all users?
3. How can we best meet privacy, security, and compliance requirements?
4. What capabilities will we need to facilitate user and entity affiliation?
5. How and where should we start — cloud first, build or buy?

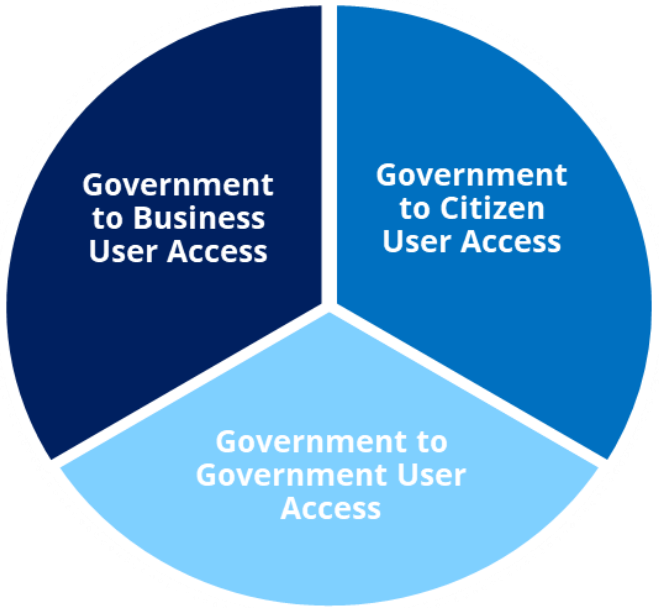
# NextGen XMS – Overview

NextGen XMS is a scalable, cloud-based identity federation broker that provides a single unified digital identity experience for HHS mission areas in the Government-to-Citizen, Government-to-Business, and Government-to-Government space.

## User Personas Supported

- External users
- Federal agency users
- Business entities
- Citizens

## Use Cases




## NextGen XMS Capabilities

- Trusted credentials via **accredited sign-in partners** or federal government issued **PIV/CAC**
- Compliance with **federal standards** (NIST, OMB, HHS EPLC requirements, etc.)
- Remote **Identity proofing** and **delegated proofing**
- **Standards-based approach** to application integration
- Configurable **access request framework**
- Business entity **affiliation management**
- **Auditing** and **Reporting**
- *Digital Identity **fraud detection** and **zero-trust** aligned **continuous authentication**
- ***FIDO2 (YubiKey security keys)** as additional authenticator

*Upcoming capabilities

# NextGen XMS – Benefits to HHS

HHS NextGen XMS delivers value to application teams and various user personas by:

Providing a **trust orchestration platform** for HHS customers and external users to **securely access** HHS platforms.

Mandating, at a minimum, **multi-factor authentication** (MFA) to access HHS applications and **improve security.**

Delivering the ability to **verify identity** of customers through **various channels** (in-person, driver's license, biometrics) with a **range of MFA options** (SMS one-time password, security key, authenticator application) to support **coverage/equity across diverse user base.**

Providing application team the ability to **customize external user workflows** to deliver the application's desired **user experience.**

Allowing net new users to **leverage existing credentials** to login, **reducing friction** during account creation.

# NextGen XMS – Ongoing Initiatives

HHS continues to invest in efforts to enhance XMS and align new implementations with federal regulations, policies, and guidance of ICAM services.

**Healthcare Proof-of-Concept**

Participating in a proof-of-concept with Carin Alliance to prove out applicability of a Digital Identity platform for federating trusted Identity Assurance Level 2 (IAL2) certified credentials across health care organizations to connect Patients, Providers and Payers.

**Multiple Sign-in Partner Options**

Continue onboarding of additional Credential Service Providers (CSPs) to improve reliability and coverage to a diverse user set.

**Adaptive and Continuous Authentication – Zero Trust aligned**

Adaptive, context aware and continuous authentication based on behavioral and risk profile.

# Q & A