



Presentation to  
House Committee on Technology:  
HHS System Identity & Access Management

---

Bowden Hight  
Deputy Executive Commissioner  
Information Technology Services  
Health and Human Services Commission

May 21, 2014

# HHS Scope & Use

---

- **Internal Users**
  - 5 Enterprise agencies
  - More than 55,000 employees
  - More than 800 locations across Texas
  - About 900 applications
- **External Users**
  - HHS Clients
  - Non-HHS state agencies
  - Federal agencies
  - Trading Partners and Business Associates
- **Goal of a secure and meaningful information exchange to clients via self service on multiple types of devices. Examples include:**
  - Eligibility workers are able to work from multiple locations.
  - Providers can validate eligibility for Medicaid and check authorized services.
  - Clients verify their identity through self-attestation. Once validated, eligible clients can receive notifications, check status of benefits and report changes in status.
  - Clients can access a 36 month history of their personal health records, request medical transportation and search for providers.
  - CASA volunteers can access portions of a foster child's case record for real time information.

# HHS Identity Access Management (IAM)

- Identity and Access Management solutions enable the right individuals to access the right resources at the right times for the right reasons.

Stores Information	<ul style="list-style-type: none"> <li>• The identity management system stores information about the following resources: applications, databases, devices (e.g. mobile phones, pagers, card keys), facilities (e.g. warehouses, office buildings, conference rooms), groups, operating systems, people (e.g. employees, contractors, customers), policy (e.g. security policy, access control policy), and roles.</li> </ul>
Authentication and authorization	<ul style="list-style-type: none"> <li>• The identity management system authenticates and authorizes both internal and external users. Upon request for access to a resource, the identity management first authenticates the user by asking for credentials, which may be in the form of a username and password, digital certificate, etc. After authentication, the identity management system authorizes the appropriate amount of access based on the user's identity and attributes.</li> </ul>
External user registration and enrollment	<ul style="list-style-type: none"> <li>• The identity management system allows external users to register accounts with the identity management system and also to enroll for access privileges to a particular resource. If the user cannot authenticate with the identity management system the user will be provided the opportunity to register an account. Once an account is created and the user successfully authenticates, the user must enroll for access privileges to requested resources. Only after the user has successfully registered with the identity management system and enrolled for access will access to that resource be granted.</li> </ul>
Internal user enrollment	<ul style="list-style-type: none"> <li>• The identity management system allows internal users to enroll for access privileges. Unlike external users, internal users will not be given the option to register because internal users already have an identity within the identity management system. The enrollment process for internal users is identical to that of external users.</li> </ul>
Password management	<ul style="list-style-type: none"> <li>• The identity management system allows for password management. Users are able to reset their own passwords and synchronize passwords across multiple systems. The IT help desk is also able to reset passwords on behalf of users.</li> </ul>
Auditing	<ul style="list-style-type: none"> <li>• The identity management system facilitates auditing of user and privilege information. The identity management system can be queried to verify the level of user privilege. The identity management system provides data from authoritative sources, providing auditors with accurate information about users and their privileges.</li> </ul>
User Self Service	<ul style="list-style-type: none"> <li>• The identity management system allows users to maintain their own personnel information and perform certain routine account tasks. For example, users can update their personal contact information, change their passwords, or synchronize passwords across all systems. If necessary, the changes can be validated before the appropriate authoritative sources are updated.</li> </ul>
Central Administration	<ul style="list-style-type: none"> <li>• The identity management system allows administrators to centrally manage multiple identities. Administrators can centrally manage both the content within the identity management system and the structural architecture of the identity management system.</li> </ul>
Delegated Administration	<ul style="list-style-type: none"> <li>• The identity management system allows delegated administration, so that administrators can manage identities for which they are responsible. Delegated administrators are not able to make any structural changes to the identity management system. Delegated administrators are only able to manage the information stored in the identity management system.</li> </ul>

## Current HHS IAM

---

- HHS has three initiatives to support automated provisioning/de-provisioning, access authorization and single sign-on services to HHS agencies:
  - Enterprise IAM – supports 23 applications from HHSC and DADS accessed by more than 8,000 users.
  - Texas Integrated Eligibility Redesign System (TIERS) IAM – supports integrated eligibility and 12 other applications accessed by more than 16,000 users.
  - Enterprise Single Sign-On (ESSO) – supports 6 applications accessed by more than 13,000 users.
- The HHS IAM solution includes:
  - High availability/redundancy.
  - Disaster recover support.
  - Support of multiple HHS agency applications.
  - Support of multiple application architectures.

# Future of HHS IAM

---

- Expand IAM services to all HHS agencies.
- Support for mobile security.
- Support for cloud security.
- Role-based provisioning.
- Support for identity federation and trust.
- Active directory integration with Enterprise IAM.

# A Statewide IAM Solution

---

- HHS would benefit from a statewide solution with the following gains:
  - Increased ability to coordinate and communicate with clients, agents and employees.
  - Easy integration with other state agencies and business partners.
  - Reduction of costs and work effort, including:
    - Eliminating more than 200 different agency solutions.
    - Minimizing time spent on interagency communications.
    - Improving security (architected into the solution).

# Lessons from HHS Implementation

---

---

- IAM requires a highly complex, multi-year implementation due to scope, number of applications, number of business partners, etc.
- Elements of a successful IAM project include:
  - Strong executive sponsorship and governance to manage the scope, prioritize applications and manage risks.
  - A project roadmap consisting of multiple “mini” projects that demonstrate an immediate return on investment.
  - Experienced, dedicated project management staff or vendors.
  - A project team with representatives from each agency, and each organization with the agency, that is being “touched” by the solution, including HR, IT, Help Desk, Training and upper-level management.
  - Proper expectations set and communicated with expectation of realistic accomplishments within a reasonable timeframe.
  - Realistic understanding of complexity of applications and internal infrastructure support processes.
  - Appropriate level of resources dedicated to the project within IT and within business areas.