



HHS Information Technology and Data Services Modernization Plan

As Required by

2020-21 General Appropriations Act,
House Bill 1, 86th Legislature, Regular
Session (Article II, Health and Human
Services Commission, Rider 175)



TEXAS
Health and Human
Services

Health and Human Services

October 2020

Table of Contents

Executive Summary	1
Introduction-Agency Overview	5
Texas Health and Human Services	5
Health and Human Services Commission	5
Department of State Health Services	6
Conclusion	6
Organizational Overview	8
HHS Transformation and Information Technology	8
Overview of HHS Information Technology	8
Information Technology Organization and Roles	9
HHS IT: Additional Roles and Responsibilities	13
HHSC Office of Performance.....	15
HHSC Office of Performance: Roles and Responsibilities	16
HHSC Office of Performance: Additional Roles and Responsibilities.....	20
10 Year Plan Approach	22
Approach.....	24
Legacy Infrastructure Modernization	28
Overview and Background	28
Current State	29
Risks.....	31
Desired Outcome and Future State	34

Timeline	36
Resources Needed	39
Benefits to Texans	40
Security	41
Overview and Background	41
Current State	42
Desired Outcome and Future State	46
Timeline	47
Benefits to Texans	50
Legacy Systems Modernization	51
Overview and Background	51
Current State	53
Desired Outcome and Future State	56
Timeline	58
Benefits to Texans	62
Data Services	63
Overview and Background	63
Current State	65
Desired Outcome and Future State	68
Timeline	72
Resources Needed	81
Identity and Access Management	82
Overview and Background	82

Current State	84
Desired Outcome and Future State	86
Timeline	88
Benefits to Texans	91
Converged Services.....	92
Overview and Background	92
Current State and Risks of Network Infrastructure Failure.....	94
Desired Outcome and Future State	96
Timeline	97
Benefits to Texans	100
Client and Agency Computing	101
Overview and Background	101
Current State	101
Desired Outcome and Future State	102
Timeline	104
Benefits to Texans	110
Workforce	111
Current State	111
Conclusion	116
List of Acronyms	118

Executive Summary

The Health and Human Services (HHS) Information Technology and Data Services Modernization Plan is submitted pursuant to Rider 175 of the 2020-21 General Appropriations Act, House Bill (HB) 1, 86th Legislature, Regular Session, 2019, (Article II, Health and Human Services Commission, Rider 175). The rider states:

175. Information Technology and Data Services Modernization Plan. It is the intent of the legislature that, not later than October 1, 2020, the Health and Human Services Commission, using money appropriated to the commission by this Act, prepare and submit to the Governor, Legislative Budget Board, and post to the commission's website a 10-year system-wide plan outlining the manner in which the commission intends to transition its information technology and data-related services and capabilities into a more modern, integrated, secure, and effective environment. The plan must:

1. Describe the commission's project management process;
2. Identify the resources required to implement the plan;
3. Define the desired outcomes of the plan;
4. Include:
 - a. Legacy system modernization or replacement;
 - b. Efforts towards server consolidation through the Department of Information Resources data services center program;
 - c. A description of cloud computing service options; and,
 - d. An analysis of the commission's technical and data architecture that is necessary to provide enhanced data analytics, reporting, and performance management need; and,
5. Describe the commission's approach to creating an automated, interoperable system-wide data analytics and performance management system that transforms data into meaningful information to support data-driven decision making, quality improvement initiatives, efficient service delivery, and effective regulation and oversight of programs administered by the commission.

The Rider 175 plan details the Texas HHS's 10-year plan for Information Technology (IT) and Data Services Modernization, including goals, objectives, deliverables, measures of success, and recommendations for each key topic area. The plan addresses information technology and data services for the Health and Human Services Commission (HHSC), Department of State Health Services (DSHS), and the Office of the Inspector General (OIG), as well as the shared technology and support services provided to the Department of Family and Protective Services (DFPS) as required under HB 5, 85th Legislature, Regular Session, 2017.

Key Points of the Rider 175 Plan

- HHS is required to ensure its systems and processes are aligned with the 2020-2024 State Strategic Plan for Information Resources Management, in compliance with Government Code, Chapter 2054; Texas Administrative Code, (TAC) Title 1, Part 10, Chapter 202; and the Texas Department of Information Resources (DIR) Software Currency Policy.
- Like most state agencies, HHSC and DSHS maintain "mission-critical" business applications for program areas that use legacy software or hardware, and in most cases, both. HHS IT must continue to modernize legacy infrastructure, by implementing enterprise IT system tools and services and applying industry standard service management processes.
- The lack of automation of program functions results in poor use of staff time and agency resources. The only option for many program and administrative employees is to manually document information (for example, creating an excel spreadsheet). This increases the risk of user error, increases processing time, and limits progress toward a model centered on sustainable and reliable data-driven management.
- In addition to the implementation of agency-wide processes and standards, HHS utilizes a variety of systems and tools to support overall IT operations like separate Help Desk solutions, disparate asset management tracking systems, and tools for monitoring and data classification.
- HHS maintains both sensitive, protected information and systems/applications that perform mission-critical functions for the state's safety net which require continuous security monitoring. Security efforts include the adoption of national standards for electronic Protected Health Information (PHI) data and Federal Tax Information (FTI).
- A modernized IT system requires modernized IT infrastructure to work optimally and deliver the benefits of increased productivity and reduced operating costs. HHS uses many obsolete and custom-developed applications

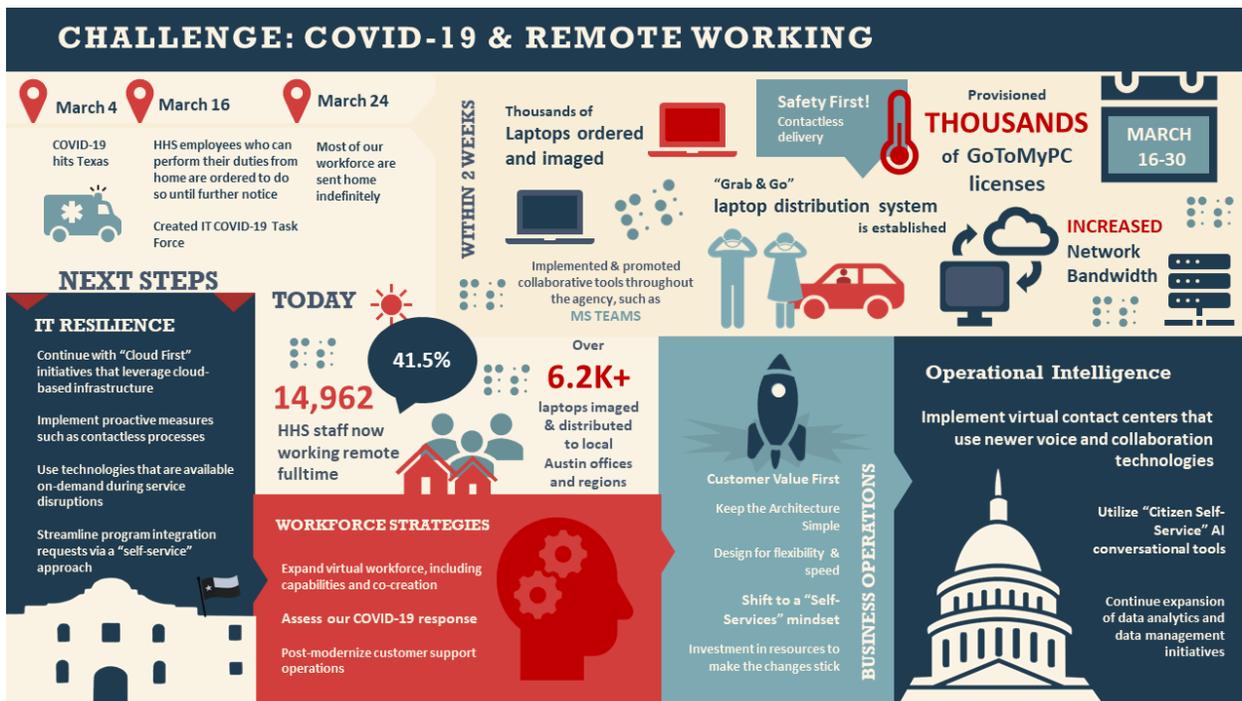
that take longer to deploy and require considerable inefficient human and technological resources to operate and maintain.

- The HHS data, performance, and analytical landscape today is largely fragmented, relying on hundreds of separate business system applications that were developed at different points in time based on specific business needs with little consideration of future data interoperability, data integration, or advanced analytics.
- The interconnected nature of technology and data creates a significant financial and operational undertaking to develop and maintain an effective environment.

With the intention to create a more efficient and secure system, the last reorganization process (also known as Transformation) established HHSC's IT oversight authority for all agency IT projects and procurements, centralized information systems, planning authority for system-wide policies and procedures, and a responsive, up-to-date security system. Four distinct agency IT departments were consolidated into one division with a variety of staff, infrastructure, systems, applications, services, and processes. The variation caused by consolidation of legacy HHS agencies resulted in a multitude of IT systems and associated architectures as well as data management processes that are not consistently complementary or aligned.

Over the last several biennia, IT leadership has consistently worked to address process inefficiencies and redundancies, update outdated policies and procedures, and remediate legacy business applications while also establishing standardized governance, project management, and exploring the use of cloud-based services to address IT needs.

HHS anticipates multiple organizational benefits with the consistent implementation of IT and data services modernization. Expected benefits include improved security and regulation of applications and platforms, advancements in quality and efficiency of service delivery, greater oversight of programs and services, and increased data integration for data-driven decisions. The infographic below demonstrates several modernization efforts that were accelerated to respond to the COVID-19 pandemic and ensure client services were continued safely and effectively.



The modernization of HHS IT capabilities will greatly benefit Texas communities and the citizens HHS serves. These benefits include advancements in responsiveness and the availability of systems that support critical program services such as Temporary Assistance for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), Children’s Health Insurance Program (CHIP), and Medicaid/ Medicare; a mature cybersecurity program that reduces security attacks and protects the personal health information of Texans; a proactive strategy to maintain critical databases for laboratory systems which contain the research information that runs our public health programs and applications that operate all client benefit eligibility for the entire state.

Controlling the spread of COVID-19 is the most critical challenge Texans face today, and HHS is committed to continuing to develop its IT capabilities to meet the strong demand for modern technology to address these challenges. For example, the implementation of telemedicine technology will allow clients to receive care at home and reduce the likelihood these high-risk individuals are exposed to the virus.

The Rider 175 plan is a 10-year roadmap which continues the work of addressing aging infrastructure, modernizing legacy business applications and systems, and automating manual processes to provide the best service delivery to Texans.

Introduction-Agency Overview

Texas Health and Human Services

The HHS system, which includes the HHSC and DSHS, serves more than 7 million people each month and affects the lives of all Texans, from the food they eat to the health care they receive. These two agencies employ more than 41,000 staff, operate a \$78.5 billion biennial budget, and manage more than 220 programs ranging from health care, food benefits, cash assistance, state in-patient psychiatric hospitals, regulation of child care, nursing and health care facilities, public health tracking and data collection, vital records, food safety, and newborn screening. Every program within the system depends on the seamless use of data and information technology to track and deliver program benefits and serve the people of Texas.

The HHS system has undergone extensive changes to its organizational structure in accordance with statutory changes made during the 84th and 85th legislative sessions and based on recommendations of the Sunset Advisory Commission issued in 2015. Transformation of the agency structure from four agencies into two, streamlined service delivery by reducing fragmentation and inefficiencies. This reformed HHS system addressed program silos by aligning similar functions, clarified lines of authority to improve accountability, and improved processes and procedures to allow for effective and efficient changes to the way HHS agencies operate.

The full consolidation of the HHS system IT staff and functions was completed in 2017. Policies establish HHS IT authority to oversee all agency IT projects and procurements as well as centralizing information systems, planning authority for system-wide policies and procedures, and establishing an IT security system that ensures minimum standards across all agencies. The HHS system is employing information technology to support specific functions and services while planning and implementing a modernized, integrated, secure, effective, and reliable work environment.

Health and Human Services Commission

HHSC is responsible for the overall delivery of hundreds of health and human services and programs across the state. It provides for those who need assistance to buy necessities, eat nutritious foods, and pay for health care costs by administering programs such as TANF, SNAP, Women, Infants and Children (WIC),

Medicaid, and CHIP. The agency operates 13 state-supported living centers (SSLCs) that provide direct services to people with intellectual and developmental disabilities and 10 state hospitals that serve people who need inpatient psychiatric care. All 23 of these facilities are operated 24 hours a day, seven days a week (24/7). HHSC also provides a multitude of other mental health and substance abuse services, help for people with special health care needs, community supports and services for older Texans, disaster relief assistance, and resources to fight human trafficking.

The Regulatory Services Division (RSD) works toward health and safety in public establishments such as medical facilities, nursing homes, child care centers, and facilities operated or contracted by the state. Supporting the divisions and areas that provide direct services to Texans on a daily basis, are numerous HHS administrative divisions including financial services, legal services, policy, performance, system support services, contracting/procurement, IT, and public affairs that ensure continuity of business operations and effective delivery of services.

Department of State Health Services

DSHS is charged with promoting and protecting public health through prevention, intervention, and effective partnerships with communities across the state. The agency helps prevent the spread of communicable diseases, tracks public health data, and protects consumers by licensing retail food establishments and stores. Key responsibilities for the agency comprise of Birth, Death, and Marriage Records Services and Public Health Services, which include Laboratory and Infectious Disease Services. The DSHS Laboratory is a unique and essential state resource that is the foundation for much of DSHS' public health work. The laboratory, one of the largest public health laboratories in the nation, performs necessary public health testing to identify, investigate, and control individual and community disease, and significant health threats. As a public health laboratory, it performs tests that no other laboratory in the state can provide. DSHS also works with local health departments to deliver public health services to communities and identify how to improve the health outcomes of populations in a state as big and diverse as Texas. The agency also responds to disasters and disease threats and outbreaks.

Conclusion

The Texas HHS system is focused on streamlining practices, limiting unnecessary expenditures, and leveraging the latest technology, agile development practices,

and innovation to maximize efficiencies and improve service delivery and outcomes for people receiving services.

Building on efficiencies gained through transformation, the HHS Information Technology and Data Services Modernization Plan outlines transitioning IT and data-related services and capabilities over the next 10 years into a more modern, integrated, secure, and effective environment. This plan outlines goals, objectives, deliverables, and measures of success that align with the HHS System Strategic Plan and system priorities. The execution of Information Technology and Data Services Modernization Plan will advance the HHS mission of improving the health, safety, and well-being of Texans with good stewardship of public resources.

Organizational Overview

HHS Transformation and Information Technology

HHS Transformation began with the enactment of Senate Bill (SB) 200, 84th Legislature, Regular Session, 2015, which directed the consolidation of the Department of Assistive and Rehabilitative Services (DARS), the Department of Aging and Disability Services (DADS), and certain administrative services from DSHS, and DFPS within HHSC. This directive resulted in the HHS Transformation effort with the goal of producing a more efficient, effective, and responsive HHS system. In September 2016, the first phase of this effort became operational, and in September 2017 the second phase was completed.

The HHS Transformation consolidated the Information Technology departments from four agencies into one division. This consolidation brought with it a variety of staff, infrastructure, systems, applications, services, and processes previously maintained in separate organizations. Consolidating these departments into one led to the endeavor to evolve and streamline many disparate legacy operations into a modern, efficient Information Technology organization .

Overview of HHS Information Technology

Mission

Provide outstanding customer service and innovative technology solutions securely, efficiently, and effectively.

Vision

Delivering exceptional customer service and solutions.

Areas of Interest

HHS IT provides integrated systems, applications, infrastructure, services, and information security support for the agency, in addition to strategic IT financial, project, and procurement support to inform data-driven decision making. As part of this goal, IT has identified four areas of focus:

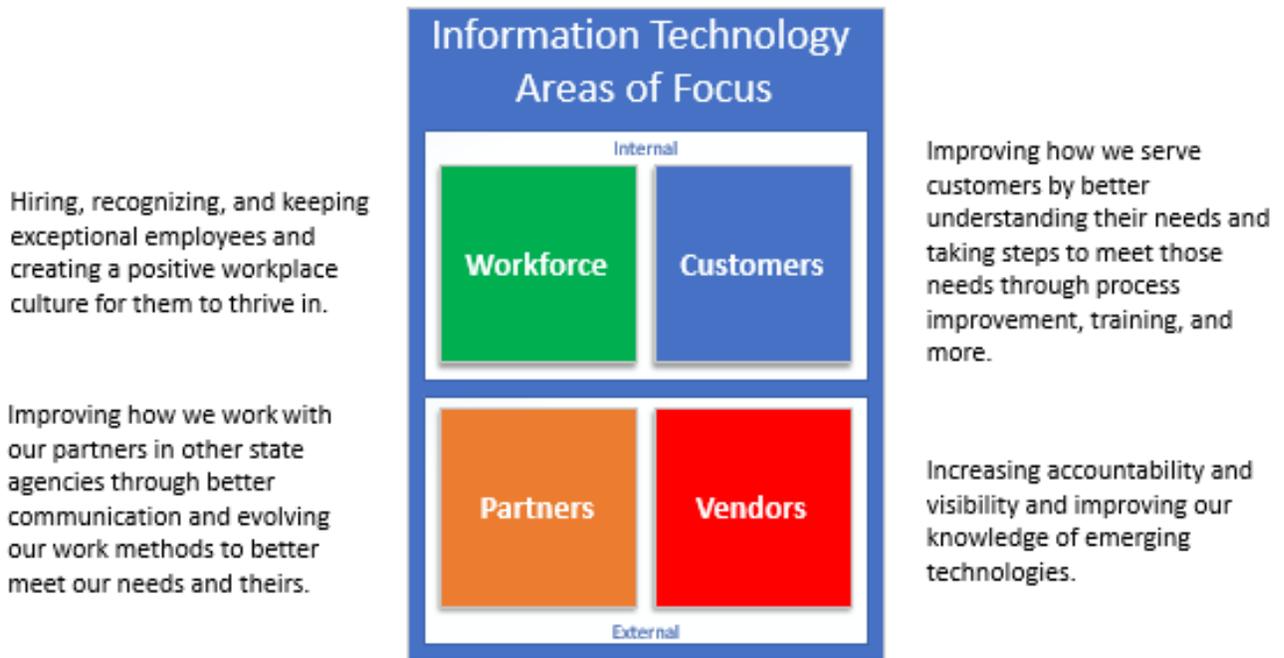


Figure 1 Information Technology Areas of Focus

Information Technology Organization and Roles

The HHS IT is divided into eight departments with distinct functions under the leadership of the HHS Deputy Executive Commissioner for IT & Chief Information Officer (CIO). Under the CIO’s guidance, these departments work closely together and partner with programs, agencies, and operational areas to drive system-wide, performance-based improvements in Information Technology delivery. The Information Technology division is organized as follows:

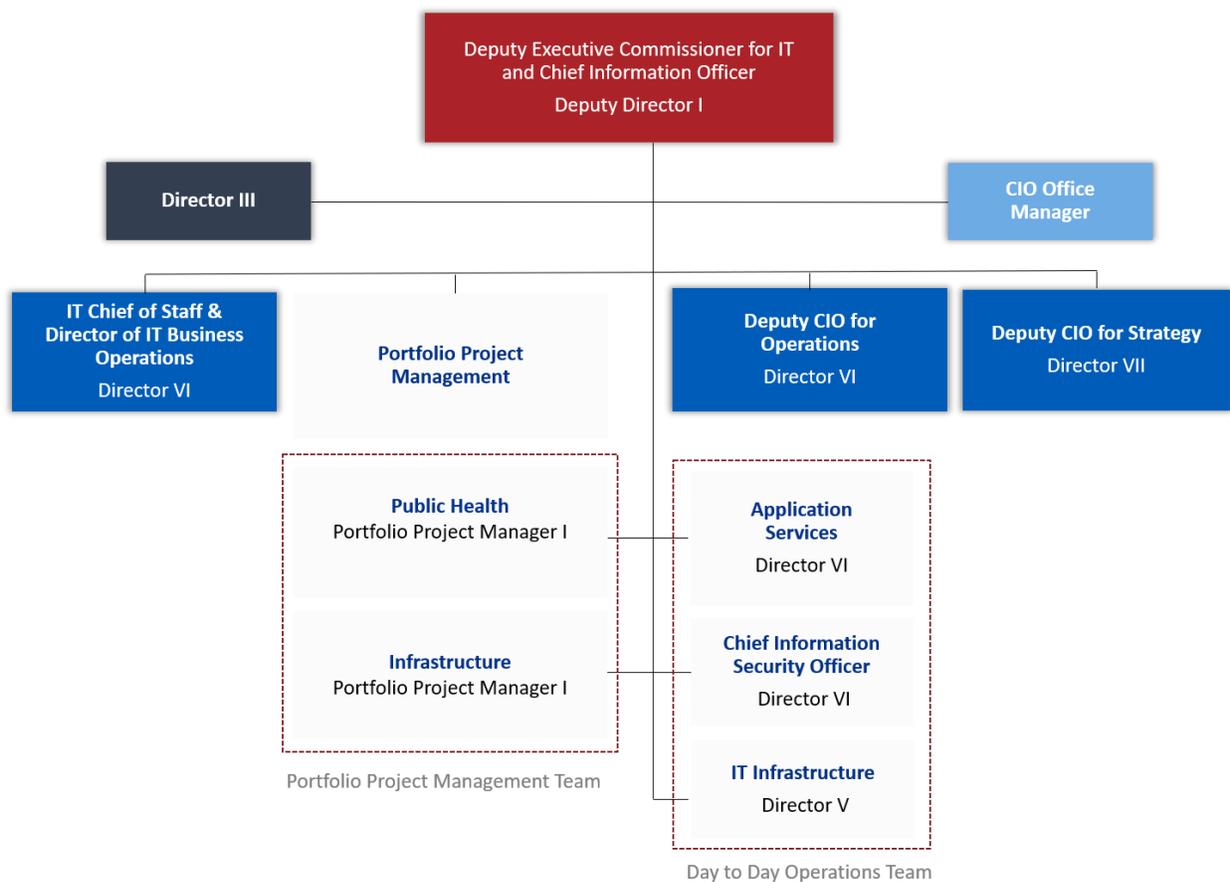


Figure 2 HHS IT Org Chart

Deputy Executive Commissioner for Information Technology and Chief Information Officer

The Chief Information Officer (CIO) is responsible for overseeing all aspects of information technology for the HHS system and keeping leadership apprised of significant issues and concerns. The CIO fulfills the role of HHSC and DSHS Information Resources Manager (IRM). Responsibilities of the IRM include, but are not limited to, overseeing the acquisition and management of the organization’s information resources; adopting and executing information resource (IR) standards, policies, and procedures as well as reporting on the IR investment and benefits to executive management, as well as state and federal executive stakeholders. The CIO is also responsible for ensuring compliance with state and federal legislative mandates; overseeing the submission of the agency’s Biennial Operation Plan (BOP); oversight of the implementation of the organization’s project management practices; and demonstrating in the organization’s strategic plan the extent to which the organization uses its project management practices.

IT Chief of Staff and Director of IT Business Operations

The Chief of Staff oversees all IT Business Operations which provides a range of independent, objective, and innovative services to support IT departments and business operations, creating operational efficiencies that comply with internal and external policies and procedures. The services provided include budget management and forecasting, contract management and oversight, federal and state reporting coordination, procurement project and contracting support, and workforce and planning/policy support.

Deputy Chief Information Officer for IT Strategy

The Deputy Chief Information Officer (DCIO) for IT Strategy monitors and oversees activities related to projects, IT business operations, data architecture, and the chief technology office. The DCIO also manages business architecture engagements using business capability modeling modalities; strategies for technology standardization, consolidation and modernization.

Deputy Chief Information Officer for Governance and Enterprise Relationship Management

The Deputy Chief Information Officer (DCIO) for Governance and Enterprise Relationship Management oversees the day-to-day activities related to infrastructure, security, and applications. The DCIO for Governance and Enterprise Relationship Management also facilitates the IT governance process and interfaces with customers and business partners to ensure effective engagement with HHS IT.

Chief Information Security Office

The Office of the Chief Information Security Officer (CISO) is responsible for coordinating and leading IT physical and logical security functions, including the strategic planning for the HHS system security program, assessing and managing technology risk, establishing and maintaining security policies, and creating a risk-conscious and security-aware culture. Operational functions include the design and implementation of a secure and resilient architecture, oversight of risk-mitigating control activities, as well as cyber security and privacy incident management.

Chief Technology Officer

The Chief Technology Officer (CTO) manages the overall technology architecture and works collaboratively with program areas throughout the agency on developing IT investment strategies and roadmaps for current and future technology solutions. The CTO responds to all new IT project requests by evaluating and recommending

rationalization of IT environments, systems, and tools with the goal of simplifying environments, increasing the speed of new technology rollouts, and reducing the total cost of ownership. Lastly, the CTO establishes the current and long-range direction of technology aimed at keeping the organization on the forefront of innovation.

Chief Data Architect

The Chief Data Architect (CDA) oversees data analysis and architecture work across the agency. The CDA provides direction and guidance in strategic operations and planning, employs expertise with innovation and ingenuity to deliver robust, enterprise-scale data platforms.

IT Infrastructure

The IT Infrastructure department provides a range of services to support the operational IT needs of the HHS system. IT Infrastructure includes four areas: Converged Services which provide telecommunication and network services; Customer Service and Support which provides service to customers across the state, records, tracks, resolves, and quantifies IT problems; IT Data Center Services and Operations which ensure HHS programs receive collaborative, focused, cost-optimized, and consistently managed data center services. The last area within IT Infrastructure is IT System Services which provides identity and access management services, hardware and software asset management and mobile service provision.

Application Services

The Application Services department provides support for HHS IT applications through all phases of the software development lifecycle from requirements to ongoing maintenance. This includes custom application development and support, as well as a large number of commercial off-the-shelf (COTS) solutions and other third-party created software. Application Services also manages systems integration among multiple applications, vendors and infrastructure.

IT Project Management Office

The IT Project Management Office (PMO) provides project management guidance and support, including process development, analysis, and training. The PMO is responsible for analyzing project data to identify trends and measures project performance and establishes policies, processes, standards, and best practices for managing IT projects.

HHS IT: Additional Roles and Responsibilities

IT Governance

HHS IT Governance defines the assignment of decision rights and related accountability for the use of information technology. Governance is the decision framework and process by which entities make investment decisions and drive business value. Goals and objectives for HHS IT Governance include:

- providing appropriate executive oversight of IT governance portfolios;
- improving accountability for results;
- investigating modern solutions to reduce risks, inefficiencies, and complexity;
- improving resource utilization through focused IT spending;
- improving system integration and interoperability;
- providing for more effective strategic planning to align IT and program customer strategies with biennial and annual plans and resources;
- clarifying roles, responsibilities and processes related to all facets of IT proceedings; and,
- ensuring the appropriate execution of modernization plans.

The HHS IT Governance model includes 6 business portfolios and 2 system-wide portfolios:

- Public Health Services;
- Administrative;
- Medical and Social Services;
- Regulatory Services;
- State Operated Facilities;
- Inspector General;
- Infrastructure and Shared Services (system-wide); and,
- Portal Authority (system-wide).

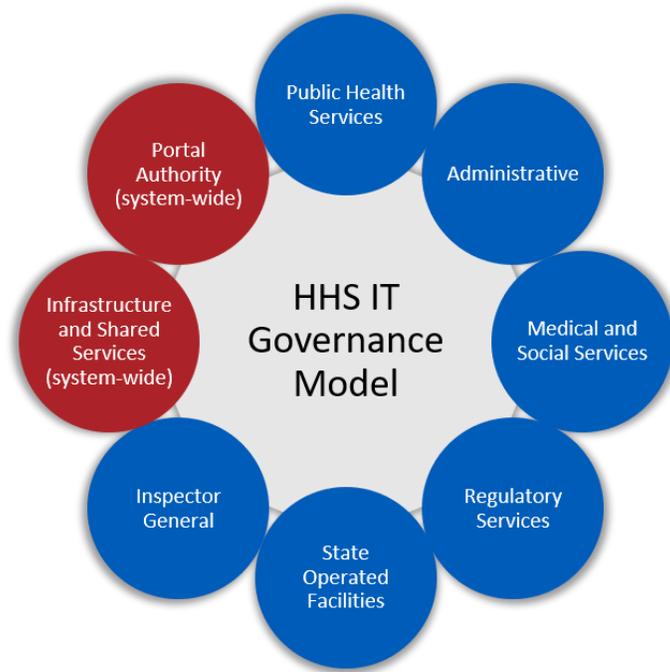


Figure 3 IT Governance

HHS IT coordinates a governance structure with representatives from central parts of the enterprise, including Business, Applications, Infrastructure, Finance, and Security, to participate in IT decisions using the IT Governance Intake Process. The process ensures that DSHS and HHSC program requests for IT services are clearly defined and that IT solutions are approved and prioritized by leadership. This structure also provides a forum for notification of IT policies to facilitate awareness and compliance, which will assist with implementing and sustaining the desired streamlined, standardized, and simplified service delivery model for IT services.

Each portfolio has an Executive Steering Committee (ESC), which includes the CIO and other members of executive management. The ESC focuses on prioritization, application and contract lifecycle planning, data analytics and ensures that program decisions are aligned with and prioritized to the HHS strategy and goals. Through the Public Health portfolio, HHS IT and DSHS collaborate in cross-agency coordination on system-wide applications and data sharing.

IT Project Management

HHS uses the DIR Texas Project Delivery Framework, utilizes well-defined internal project management processes, and employs project management professionals with extensive experience to support the delivery of high-quality products to our customers. The project management life cycle used by the agency consists of the

initiate, plan, execute, monitor and control, and closing phases. These phases provide the necessary framework to methodically define, design and develop, test, and release functionality to agency customers.

In addition, the agency has published supplemental processes to the Texas Project Delivery Framework to ensure all aspects of the project management life cycle is supported by clear and concise process documentation. These supplemental processes define the agency requirements to execute the project strategies (e.g., change management, project status reporting, lessons learned process, escalation of risk and issues, cost management, and vendor performance management). Most importantly, the agency's strategy to enhance and maintain project management practices is embodied in policies and procedures. Through continuous improvement and innovation, the agency delivers the best possible products and services through the use of the Texas Project Delivery Framework, project management professionals, defined best practices, and measuring progress and outcomes to improve our performance.

HHSC Office of Performance

HHS Transformation was also responsible for the creation of the Chief Policy & Regulatory Officer (CPRO) in March 2018, created to oversee the Transformation, Policy & Performance, and RSD. The Policy & Performance team was divided into two separate divisions the: Office of Policy & Rules and the Office of Performance (OP), to allow each area to focus on policy development, and performance management and data analysis, respectively. Since its establishment, OP has supported, expanded, and streamlined the effective use of data, analytics, and performance management across the HHS system.

OP is one of five offices with distinct functions under the leadership of the CPRO. Under the CPRO's guidance, these offices work closely together and partner with programs and operational areas to drive system-wide, performance-based improvement. HHSC established an executive level office to oversee and coordinate policy and performance efforts across the system, and each office within CPRO performs functions that support this mandate.

Led by a Deputy Executive Commissioner, OP provides integrated data analytics and measurements necessary to support decisions and identify areas for improvement. OP is also charged with the development of a secure, transparent, accessible, and reliable performance management and data analytics system. While OP is divided into three departments, these departments work seamlessly together to fulfill the OP mission and vision.

Mission

Support the HHS system strategic priorities and improve the well-being of Texans by transforming data into meaningful information to support policy decisions, innovation, and improvement initiatives and through the design, development, and maintenance of a holistic and interoperable data analytics and performance management system.

Vision

Provide ready access to intuitive, holistic, automated data analytics and performance management information resulting in coordinated, efficient and effective use of public resources.

HHSC Office of Performance: Roles and Responsibilities

OP's three departments support HHS programs, divisions, and agencies as they provide efficient and effective services to Texans, and drive data-driven decision making.

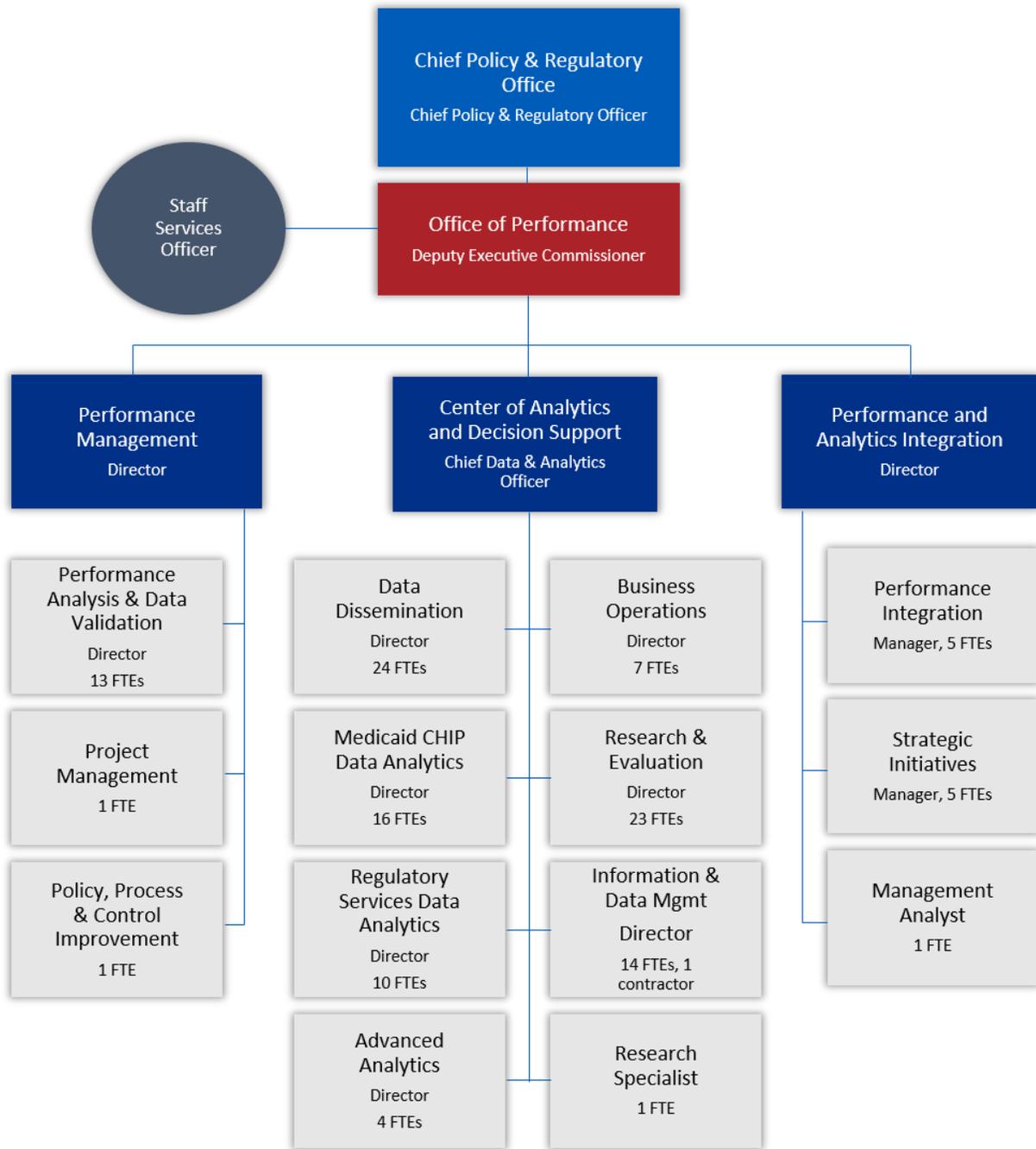


Figure 4 Office of Performance Org Chart

- Chief Policy & Regulatory Office – Chief Policy & Regulatory Officer
 - Office of Performance – Deputy Executive Commissioner
 - ◇ Staff Services Officer
 - Performance Management – Director

- Performance Analysis & Data Validation – Director, 13 FTEs
- Project Management – 1 FTE
- Policy, Process, & Control Improvement, 1 FTE
- Center of Analytics and Decision Support – Chief of Data & Analytics Officer
 - Data Dissemination – Director, 24 FTEs
 - Medicaid CHP Data Analytics – Director, 16 FTEs
 - Regulatory Services Data Analytics – Director, 10 FTEs
 - Advanced Analytics – Director, 4 FTEs
 - Business Operations, Director, 7 FTEs
 - Research & Evaluation, Director, 23 FTEs
 - Information & Data Mgmt – Director, 14 FTEs, 1 contractor
 - Research Specialist – 1 FTE
- Performance and Analytics Integration – Director
 - Performance Integration – Manager, 5 FTEs
 - Strategic Initiatives – Manager, 5 FTEs
 - Management Analyst, 1 FTE

Center for Analytics and Decision Support

The Center for Analytics and Decision Support (CADS) is responsible for data quality, strategic use and management of data, analytical support, research, data reporting and program evaluation for HHSC, as well as analytic and quantitative research on program utilization, demographic trends, and enrollment patterns for the state’s HHS programs. CADS is also charged with data governance that includes the development, use and appropriate sharing of data and data systems. CADS provides quantitative data analysis and reporting, data dissemination and data management.

- Provides data and analytical support to Medical and Social Services programs (Medicaid & CHIP Services (MCS), Access & Eligibility Services (AES), Health Developmental & Independence Services, and Intellectually & Developmentally Disabilities – Behavioral Health Services (IDD-BHS).
- Generates monthly program statistical reports, including monthly counts of SNAP recipients by zip code and demographic characteristics, or monthly counts of the number of Medicaid children visiting pediatricians, per provider.
- Responds to ad hoc requests for data-related information from the Office of the Governor, the Texas Legislature, the Legislative Budget Board, and other state agencies .

- Evaluates cost/trend analyses of client benefits, as well as trends related to the changing structure and utilization of client services.

CADS provides research and evaluation of health and health care related issues. This includes but is not limited to studies requested by the Office of the Governor, Legislature, or HHS leadership and evaluation of HHS divisions and departments, support and consultation in evaluation design, and grant, federal, or HHS-directed evaluations.

For MCS, CADS provides contract monitoring tools, including but not limited to assistance with generating and refreshing dashboards, automating contractor deliverables to the extent practicable, establishing performance measure methodologies, and providing related technical consultation for contract oversight. Additionally, CADS conducts targeted research and trend analysis on areas of high utilization, cost, or potential anomalies and provides the data and data analytics necessary to understand the potential impact of proposed policy and program changes on enrollment and utilization levels.

Performance Management

The Performance Management (PM) department is responsible for gathering, measuring, and evaluating performance measures and accountability systems, developing new and refined measures, and establishing targeted, high-level metrics capable of measuring and communicating overall performance achievement to internal and external audiences.

PM is also charged with conducting business processes analysis, measure construction, report design, training, and program consultation required to develop and maintain dashboards and reporting systems.

Performance and Analytics Integration

Performance and Analytics Integration (PAI) is responsible for identifying, coordinating, and implementing individual internal, program, and system-wide strategic initiatives that promote the effective use of data, analytics and performance management. PAI provides consultation and support to HHS staff and leadership to identify and develop cross-division and cross program outcome measures and goals. PAI also works to implement consistent process and quality controls across OP.

For performance and analytics projects and initiatives, PAI may provide services such as project leadership or management. These services may support all project phases ranging from inception, scoping, approval, implementation and close out.

As a part of this work, PAI coordinates HHS Business Plan activities and provides consultative services to HHS on strategic and operational measure development. OP consults with division leadership to identify, develop and implement projects to integrate performance measures and analytics for specific business areas or across the HHS system. As a result of this work, PAI may provide reports and deliverables that include recommendations for HHS executive leadership consideration.

HHSC Office of Performance: Additional Roles and Responsibilities

Data Governance and Performance Management Leadership

OP provides governance of HHS data assets including data quality, master and metadata management, and the strategic use of data and data sharing.

The Data Governance and Performance Management (DGPM) ESC and Council is an executive level structure that was established in August 2019. The purpose of the DGPM Program is to provide executive-level support and guidance to strategically align and direct long-term HHS initiatives, policies, and procedures related to data governance, data interoperability, data quality, data analytics, and performance measurement and management.

Chief Data & Analytics Officer

The Chief Data & Analytics Officer (CDAO) determines the strategy for analytics as a key business discipline to enhance decision making for improved business outcomes within HHS, and is responsible for information strategy, data governance, analytics control, policy development and effective exploitation of data asset. The CDAO works with HHS leadership and senior management (both within program and IT) to ensure an understanding of the interdependencies and impact point created by standardized and singular data assets on key business processes.

The CDAO position is instrumental in managing the change (to people, process, and technology) resulting from the creation of key data assets impacting key business processes. The CDAO collaborates with data trustees, owners, and stewards to support data management initiatives and ensures sustaining processes are aligned

with the strategic business objectives of HHS. The CDAO also supports compliance with system data policies and audit of data for regulatory requirements.

10 Year Plan Approach

HHS is required to ensure its systems and processes are in alignment with the goals outlined in the [2020-2024 State Strategic Plan for Information Resources Management](#), and are also in compliance with [Government Code Chapter 2054, TAC Chapter 202](#), and DIR Software Currency Policy.

In 2015, HB 2641, 84th Legislature, Regular Session, 2015, was enacted mandating that all HHS systems have the capability to transmit PHI to healthcare providers in accordance with data exchange standards developed by an accredited Standards Development Organization or with the standards applicable to electronic health records. HHS submits a biennial Health Information Technology progress report detailing compliance with these standards.

Most recently, the passage of HB 3875, 86th Legislature, Regular Session, 2019, requires HHS to ensure that when purchasing an automated information system or a major information resource project, that the system or project is fully capable of being deployed and running on cloud computing services. This requirement is a cornerstone of this plan.

In 2015, the legislature enacted SB 200 and SB 208, (84th Legislature, Regular Session), requiring transformation and consolidation of legacy HHS agencies. This consolidation resulted in a varied landscape of IT systems and associated architectures that are not always complementary or otherwise aligned. While the agency has worked diligently to ensure that the existing infrastructure reliably support organizational and program needs, as technology continues to rapidly evolve, many HHS IT systems have become difficult to support and are often inefficient, resulting in high operational costs. Upgrades and modifications – if available – are complex and expensive. Left unchecked, these challenges could put HHS operations and service delivery at risk, which can lead to poor outcomes and experiences for agency stakeholders, partners, and providers. Common hindrances can be categorized as follows: Limited Interoperability – Systems often lack the ability to share data or interact with one another, which gives rise to subsequent issues that limit the ability of HHS to fully serve constituents.

- Difficulty in Implementing Upgrades or Modifications – The rigidity of agency infrastructure – particularly those components that have exceeded the typical life expectancy – often result in relatively minor system modifications taking a prolonged period of time to complete. More problematic is the model of business processes being designed and developed to accommodate (or

circumvent) systems limitations, rather than having the requisite technology and infrastructure in place to augment and support optimal and efficient business and operational practices. Updated software and new technologies deployed to help make service delivery more effective and efficient are of no benefit if the underlying infrastructure – the foundation upon which the “house” is built – has not also been upgraded.

- Limited Reuse – HHS and the legacy agencies have been inhibited by the lack of a comprehensive technology platform strategy, which would have contemplated the development and disposition of agency assets. The result has been a significant variance in the quality of IT platforms and support across HHS programs, which leads to increased costs for the agency and inefficiencies that ultimately impact agency constituents, partners, and providers.
- The inability to design and sustain a modern infrastructure, interoperability, and integration across the agency’s technology platforms undermines efforts to unlock the value in data through outcome-oriented performance management. Providing organizational support and investment in infrastructure for these activities is essential.

Real time, data-driven decision making requires consistent and accurate recording of relevant data, leveraging processes that should be automated. Unfortunately, many programmatic and administrative business actions are recorded manually (e.g., creating a spreadsheet in Microsoft Excel) which can lead toward a greater propensity for error during transmission, while also seriously limiting the ability for HHS to move toward a model centered on sustainable and reliable data-driven management. Gaps and lags in data reporting impede the ability of HHS to align the decision-making process with the most current and accurate information available at a given time. Implementing modern technology, coupled with an agile development and operational platform will enable HHS staff to accurately record and access real-time data, and subsequently support the level of data-driven performance management expected by all stakeholders.

Technology evolves with very high frequency, and needs are often difficult to assess and price. Ensuring seamless service delivery to clients requires agency leadership to have the flexibility and authority to quickly take actionable steps to address issues concerning IT and data processing, even when the expenditures are significant. Such decisions should be made in accordance with all applicable policies, procedures, and laws in an effort to promote transparency, while also being subject to an after-action review process for identification of any issues – latent or otherwise – that arose.

Approach

The interconnected nature of technology and data creates a significant financial and operational undertaking in terms of developing and maintaining a modern environment. In addition to securing the foundational resources needed for future growth, flexibility and innovation in the design, development, operation, and financing of agency technology and data assets will be required. HHS will modernize IT and data services in four phases. While each phase is distinct, there are likely to be a number of concurrent initiatives underway at any given time, particularly as one phase nears completion and gives way to the next.

HHS IT and Data Services Modernization Plan

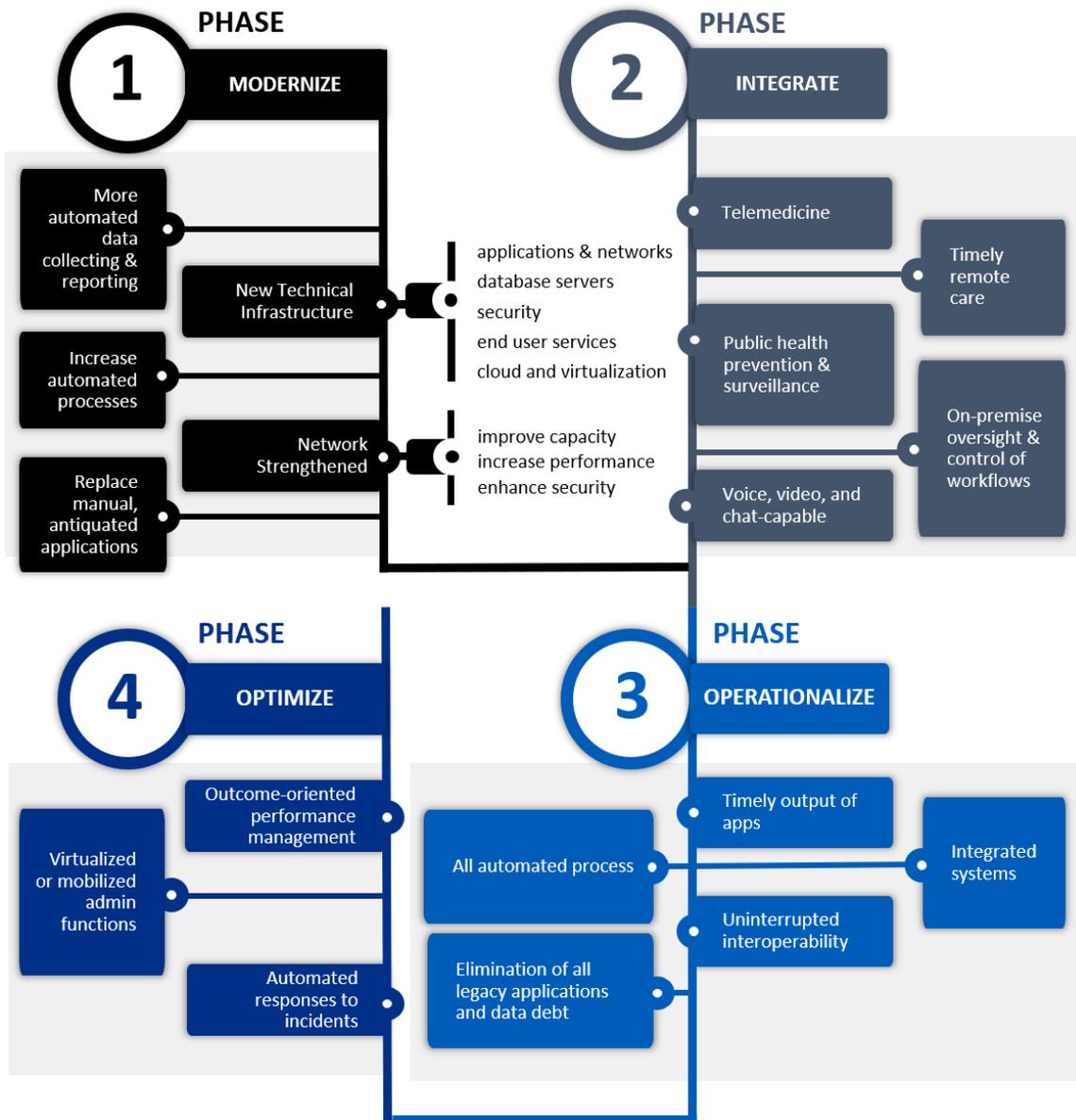


Figure 5 HHS IT and Data Modernization Plan

Phase 1 is currently underway, as HHS seeks to modernize and improve network capacity, performance, and security. Network performance is a key component of the technology and data infrastructure that directly impacts all systems, applications, and users. Staff and clients both often overlook network functionality until systems and applications fail to perform or data becomes unavailable. Mobility

and user-experience are also heavily reliant on network performance. Telemedicine and remote care- recently expanded during the COVID-19 pandemic - are service-delivery models that require a robust network.

HHS must continue to invest in the automation of data collection and reporting, including application modernization and the development of new applications that will supplant the manual management of programs and services. In the pursuit of maximizing value for clients, HHS needs flexible financing options for data governance and performance management.

Phase 2 employs a statewide technical infrastructure – inclusive of an increase in network capacity and data storage - that is reliable and highly responsive to HHS needs for: remote care; telemedicine; on-premise oversight and control of workflows; and public health prevention and surveillance. This provides the foundation to connect medical and social services with public health data for timely action and policy-making.

HHS will provide client support over voice, video, and text chats, while simultaneously protecting and securing data and client privacy. Adequate appropriations will provide HHS leadership with the flexibility to plan and respond to business demands without delay.

In the ideal environment, Medicaid information systems will run on a flexible and responsive IT platform that will reflect provider and client needs at or near real-time. Implementation of policy decisions will not require lengthy and expensive reprogramming and security workarounds; in contrast, service delivery and program oversight will be more responsive and better aligned with stakeholder expectations.

Modernized remote healthcare delivery systems and technology will be implemented in facilities operated by Health and Specialty Care Systems. Providers (HSCS) and staff will be positioned to deliver timely services that are in line with the appropriate standard of care for clients served in HHS facilities. Remote access to case management systems will also improve information sharing once a client is able to transition back into the community.

Phase 3 will see HHS free of legacy technology and data debt. Modern computing, storage, network, security, and application technology will become operational, with the decision-making flexibility and financing options available that will allow HHS to keep pace with future technological advances. The HHS IT environment will be positioned to assess, plan, develop, and deploy solutions without the latency that disrupts business and client needs.

Agile IT operations will allow HHS staff to access a full suite of technology and data tools on an as-needed basis with appropriate controls and access management in place to monitor and report on utilization. Network speeds and capacity will not impede access to these resources.

Business processes will be largely automated, and actions will be systematically captured in integrated applications that allow for customized case management and strong administrative oversight. The data collected will feed performance management and analytics tools that drive value and public benefit through outcome-based measurement and reporting.

Phase 4 envisions technology that enables nationwide virtual and/or mobile service delivery and program administration for all clients and stakeholders. These connections will include proactive, wrap-around security where detection, defense, and enhancements are automated and transparent. All applications are easily modified, and modifications are only necessary when cost and timing present a clear value proposition.

Outcome-oriented performance management is largely automated and transparent to both HHS staff and external stakeholders. Technology such as computer processing power, storage, network infrastructure, and software are developed and operated in an environment that enables such technology to operate at optimal capacity, leveraging full capabilities to remain responsive to business and client needs. Security is preventive, and artificial intelligence enables automated bolstering of the environment.

With countless challenges and demands in a rapidly changing health and human services environment, HHS is committed to utilizing modern and effective IT systems and infrastructure to increase efficiency, limit unnecessary expenditures, streamline processes, and align technical capabilities to better serve Texans.

Legacy Infrastructure Modernization

Overview and Background

The HHS IT Infrastructure Services support the operations and maintenance of over 6,000 servers and a legacy mainframe¹ environment.

The HHS IT infrastructure system hosts over 300 business applications; these applications include a variety of statewide case management systems, content management solutions, databases, business data analytic and reporting systems, administrative and collaboration systems, and system support tools. Access to these systems happens across a complex and intricate network spanning across multiple HHS campuses, health service regions, regional field offices, SSLCs, and state hospitals.

HHS IT Infrastructure Services oversees the procurement, operations, and maintenance of all local data center facilities and system administration responsibilities to include: operating systems management, database management, system security services, backup and recovery services, and disaster recovery planning and testing. These systems also leverage various infrastructure support models, ranging from HHS IT Infrastructure-managed, program-managed, and third-party vendor-managed solutions.

HHS IT must continue to modernize legacy infrastructure, by implementing enterprise IT system tools and services and applying industry standard service management processes². These modernization efforts will enable HHS IT to provide reliable, scalable, integrated, and secure infrastructure services supporting critical healthcare applications. Additionally, a modernized infrastructure supports a robust level of functionality and resiliency that is expected by the citizens of Texas when utilizing various systems including: the Texas Integrated Eligibility Redesign System (TIERS) to apply for benefits, the Medicaid Management Information Systems (MMIS) to seek health services, the Texas Electronic Vital Events Register (TxEVER)

¹ A mainframe is a large, physical, specialized computer that was developed by IBM in the 1970s to process large amounts of transactional data and act as a database management system.

² Service management services refers to the entirety of activities – directed by policies, organized and structured in processes and supporting procedures – that are performed by an organization to design, plan, deliver, operate, and control IT services offered to customers.

to process Vital Records requests, or the National Electronic Disease Surveillance System (NEDSS) to process critical COVID-19 infectious disease information. These modernization efforts will increase the security of HHS client data, provide the functionality expected by individuals who interact with HHS and give HHS the ability to provide services to clients more efficiently by using technology that is responsive to the needs of the citizens of Texas.

The full consolidation of HHS IT personnel and assets was completed in 2017. It included the continued ownership, management, and operations of HHSC infrastructure, the absorption of all DARS and DADS local and remote infrastructure, and the agreed management and operations of the DSHS local and remote infrastructure.

HB 1516, 79th Legislature, Regular Session, 2007, required Article II agencies to begin consolidating servers and mainframe environments within the state's Data Center Services (DCS) Program. During this time, HHS agencies worked individually with DIR to plan for server consolidation and virtualization efforts, which included:

- Servers eligible for consolidation to the state data center.
- Servers unable to consolidate to the state data center due to performance over a network.
- Exempted HHS managed servers.
- Exempted Third-party managed servers requiring long-term contract transition plans.

Current State

Server Consolidation

In partnership with DIR, HHS IT consolidated over 20 percent (1,200 servers) of the environment into the state's DCS program. While the DCS service providers manage these servers, some servers remain at the HHS headquarters and remote office locations while modernization efforts are underway.

HHS IT remaining 80 percent of the servers are either managed by HHS or a third-party vendor. Please see the current breakdown of HHS server management environments below:

DCS Managed Servers

- 813 server instances consolidated into the state data center or public cloud environments; and,
- 534 servers that are managed by the State DCS Providers but are approved as temporary leave-behind servers requiring wide area network (WAN) application optimization and migration into the state data center or public cloud environments.

HHS Managed Servers

- 932 exempted HHS IT managed servers requiring extensive application optimization and migration into the state data center or public cloud environments.

Outsourced Vendor Managed

- 3,360 exempted third-party managed servers requiring long-term contract transition plans–TIERS; and,
- 750 exempted third-party managed servers that require short-term contract transition plans–Texas Medicaid & Healthcare Partnership - Medicaid Management Information System (TMHP MMIS).

HHS Technology Currency³

IT infrastructure and server software can maintain optimal performance if refreshed per industry standard lifecycles. The technology currency planning methodology is based on industry best practices and DIR's Shared Technology Services hardware currency program. This program considers acquisition strategies leveraging legislative biennial funding cycles and a 20 percent staggered implementation schedule to ensure systems are proactively refreshed based on a five-year life cycle. In previous years, HHS IT Infrastructure performed reactive upgrades upon notification of a need from the Application Development team or HHS program areas. With HHS Transformation, there was a recognition that a proactive and collaborative effort is required when conducting refresh planning activities. HHS IT is working to improve this effort with participation from the business programs, application support, cybersecurity, finance, and IT infrastructure teams. This work will result in parties gaining alignment in understanding business drivers, application requirements, understanding security risks, and adhering to strategic

³ Technology Currency: the ongoing process of understanding how current an item of hardware or software is, compared to the latest available version.

goals. It will also establish long-term financial forecasting allowing HHS IT to be responsive to the needs of those who work with and rely on HHS.

Service Management, Operations, and Tools

As a result of HHS Transformation over the years, HHS IT inherited a variety of management processes used to support legacy infrastructure environments. Establishing standards and referenced architecture is a challenge as HHS IT continues to support legacy applications that require multiple types of software to function. In addition to processes and standards, HHS utilizes a variety of systems and tools to support overall IT operations. HHS has implemented separate Help Desk solutions, disparate asset management tracking systems, and tools for monitoring and data classification. By modernizing the infrastructure and moving into DIR's DCS Program, HHS will be using a standard set of referenced architecture, hardware monitoring tools, an integrated service desk and service catalog portal, a centralized asset management database, standards security controls and practices, and established service management tools and processes.

Risks

Without these modernization efforts, HHS will continue to experience risks associated with availability, security, service management, and costs.

Availability

When services experience unexpected outages, clients may experience delays when applying for on-line health benefits or receiving critical care from our SSLCs or state hospitals. Unexpected outages with systems such as NEDSS may also directly impact the health and safety of our citizens as delays could occur with reporting, laboratory testing, diagnosing, and treating chronic and infectious diseases, such as COVID-19 pandemic.

Providing current, reliable, and scalable IT infrastructure is required when ensuring the highest level of system availability.

- Outdated hardware can result in an increased number of unexpected outages, limited available parts, and limited hardware support maintenance agreements.
- Unsupported software can lead to incompatibility with newer application software, limits the ability to increase functionality, may cause hardware to malfunction, and, most importantly, the inability to apply critical security updates or software patches.

- Non-virtualized environments are unable to provide resiliency and scalability when the system experiences peak capacity.

Security

HHS IT has implemented the national standards that regulate the protection of our clients' sensitive and regulated data such as electronic PHI data and FTI. Systems containing PHI data, including but not limited to, NEDSS or TIERS, require physical and technical security controls to be put in place by maintaining hardware and software currency. These security controls are validated through regularly scheduled security assessments and audits and are subject to compensating controls in cases where standard security controls cannot be applied. Without these protections, security breaches of these systems could result in risk for disclosure of client personal health information to the public.

- Outdated hardware can lead to security vulnerabilities when firmware updates cannot be applied.
- Unsupported software can result in unpatched vulnerabilities, allowing hackers to exploit.
- Unsupported hardware and software preventing up-to-date security tools and encryption capabilities may result in extraneous or non-standard compensating controls.
- Systems hosting private and sensitive data are subject to regulatory compliance and rigorous audits.

Service Management

Leveraging the core systems and tools, HHS IT will be able to implement an integrated service management environment to support Agile and DevOps practices, which are critical in providing seamless delivery of applications and services. Modernizing these processes and tools will allow HHS IT to drive value as automation and orchestration are used to implement new infrastructure and applications. It will enable proactive monitoring and the ability to perform self-healing incident management and provide change and code release management integrated with a single asset and configuration management database. Without implementing these core systems and enabling an integrated service management environment, HHS customers will continue to experience delays in application deployments and service management activities, including:

- Reactive incident monitoring and incident management contributes to extended outages due to manual escalations and notifications.

- Non-automated server builds requiring several weeks or months to implement.
- Traditional change management practices that are out of alignment with DevOps streamlined processes.
- Disparate and non-integrated asset and configuration management systems make it challenging to identify and monitor a full inventory of infrastructure.
- Lack of a standardized data tagging tool prevents the ability to accurately identify, classify, and protect, sensitive data.

Costs

There are significant financial risks if legacy infrastructure is not up-to-date and there is a delay in modernization efforts. Hardware and software that is at End of Life or in limited support status can result in many unexpected direct and indirect costs to the agency as well as costs to citizens funding these services.

- Aged and/or unsupported hardware and software can result in premium-priced maintenance support agreements. When systems are aged, many vendors do not invest resources in developing upgrades or patches and charge higher than usual prices for extended or limited support maintenance agreements;
- Aging infrastructure is more likely to result in unexpected outages, resulting cost associated with loss of productivity for program staff, potential data loss and recovery efforts, acquiring premium-priced niche support vendors or contractors, and other possible expenses related to parts and labor, and resolution;
- Legacy environments with no modernization path can result in stranded assets and costs associated with hiring personnel or contractors;
- Multiple software versions are difficult to consolidate services and shrink costs associated with expensive software license agreements, overall resulting in redundant costs for similar services;
- The inability to accurately identify and classify data requires building all systems using the highest level of data retention requirements, resulting in uncontrolled storage growth and management costs;
- Redundant legacy systems can result in extraneous hardware and software licenses costs, as well as operating expenses for support personnel; and,

- Unsupported infrastructure and software may result in security vulnerabilities, resulting in potential penalties, audit findings and the potential loss of funding for programs.

Desired Outcome and Future State

The HHS IT and Data Services Modernization Plan's basis relies on continuing with "Cloud First" modernization initiatives that leverage cloud-based infrastructure by providing agility, cost benefits, and improved Cybersecurity hygiene⁴ and posture⁵. The overall plan projects 80 percent of the environment is either cloud-capable or leverages cloud computing environments. The other 20 percent of the environment will be reserved for systems unable to exist in a cloud.

Leveraging cloud computing environments and cloud services is crucial for providing modern healthcare systems and experiences for our clients and providers. By utilizing cloud technology, IT applications can be developed to take advantage of the cloud's flexibility and scalability necessary in providing reliable services, especially during times of crisis when families need our help the most.

This technology can also support an improved user experience for families applying for health benefit services, streamlining the request of vital birth and death records, patients receiving care at state hospitals, or providers requesting laboratory testing services for chronic and infectious diseases.

These improvements will be accomplished by providing:

- Highly reliable IT infrastructure and software;
- Continuous adherence to safeguarding sensitive and regulated citizen data;
- Enterprise secure data sharing and exchange systems;
- Consolidated case management systems with robust workflow and process management;
- Enterprise document and content management systems, with the ability to reduce print and physical mail;
- Enterprise database management systems;
- Enterprise data analytics and reporting system; and,

⁴Cybersecurity hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security.

⁵Cybersecurity posture refers to an organization's overall cybersecurity strength and how well it can predict, prevent, and respond to ever-changing cyberthreats.

- Integrated human resources and administrative management systems.

The 10 Year strategy to migrate to cloud-based infrastructure will also consider the need to support legacy HHS environments while enabling capabilities to support emerging technologies such as; modular application design concepts (e.g., containers and microservices), Artificial Intelligence (AI), Chat Bots and Robotic Process Automation(RPA), Internet of Things (IoT), and Big Data.

Additionally, HHS IT will modernize infrastructure and application support practices by implementing an integrated service management environment leveraging the HHS Business Enablement Platform (BEP) core services and tools, to include:

- Integrated Incident Management, Change Management, Event Management, Problem Management, and Release Management tools and practices.
- Consolidated application and infrastructure monitoring tools;
- Automation build tools for auto-provisioning and server security hardening;
- Data tagging and classification tools;
- Identity Access Management tools; and,
- Standard reference architecture.

Timeline

This section briefly describes some of the critical components, milestones, and resources planned over each biennium to drive HHS IT’s legacy infrastructure modernization efforts.

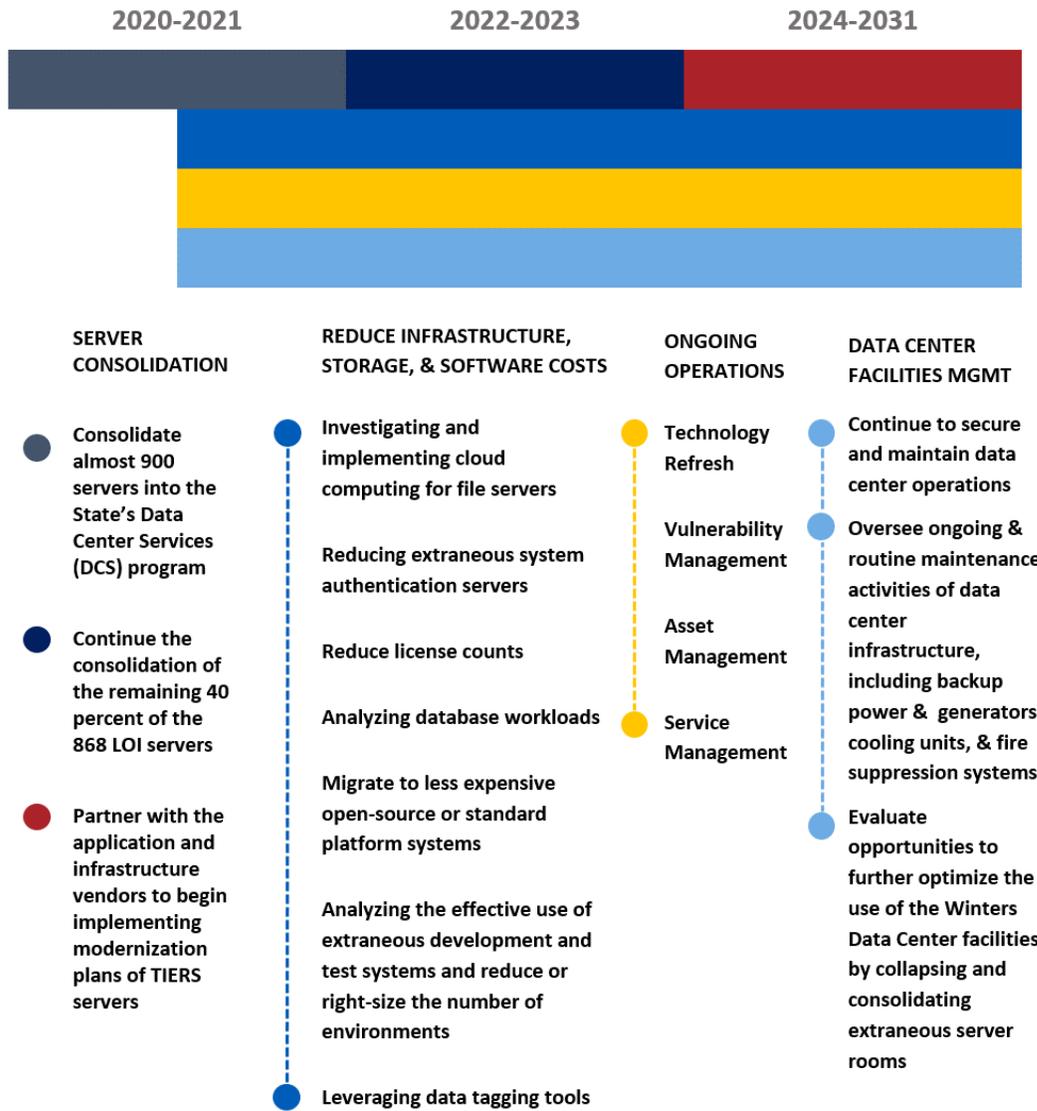


Figure 6 Infrastructure Timeline

Server Consolidation

Fiscal Years (FY) 2020 - 2021

With the funding provided by the 86th Legislature, efforts are currently underway to consolidate almost 900 servers into the State's DCS program. These efforts will ensure that the legacy equipment is in a modern virtualized private community cloud environment with up-to-date hardware infrastructure, expandable storage, tapeless backup and recovery systems, disaster recovery, and managed using federal security controls. These servers support the following applications:

- Medicaid Management Information System (MMIS);
- Laboratory Information Management System (LIMS);
- Blood Lead Surveillance System Efficiency (BLSSE);
- NEDSS; and,
- Local Office Infrastructure (LOI) servers.

TIERS has an exemption from the DCS program for a minimum of five years. However, the HHS IT Infrastructure teams will be working with third-party vendors to assess the viability for TIERS to be cloud-enabled.

FY 2022 - 2023

Continue the consolidation of the remaining 40 percent of the 868 LOI servers. TIERS to remain under a DIR DCS exemption but continue legacy modernization planning efforts with the vendor.

FY 2024 - 2031

As TIERS servers remain under a DIR DCS exemption, HHS IT Infrastructure will partner with the application and infrastructure vendors to begin implementing modernization plans. These plans involve implementing cloud-like technology and/or migrating to the cloud, overall enabling the benefits of flexibility and scalability offered through cloud computing.

Service Management, Process, and Tools

FY 2020 - 2031

HHS IT Infrastructure will leverage the BEP's core services and tools. These services and tools will be implemented in a phased approach. They will allow core service delivery capabilities to include: automation and orchestration used to implement new infrastructure and applications, data tagging and classification, proactive monitoring and performance of self-healing incident management, and provide change and code release management integrated with a single asset and configuration management database.

Reduce Infrastructure, Storage, & Software Costs

FY 2021 - 2031

HHS IT Infrastructure modernization plans consist of investigating ongoing cost optimization strategies. These strategies include:

- Investigating and implementing cloud computing for file servers, overall reducing the costs associated with storage, maintenance, and backup of large volumes of data;
- Reducing the number of extraneous system authentication servers (e.g., Domain Controllers);
- Reviewing and validating software needs and reducing license counts when possible;
- Analyzing database workloads to ensure HHS IT is leveraging appropriately powered relational database systems by reserving workloads running high online transactional processing or large data warehousing to more industrial-strength systems versus less costly database systems used for general workloads;
- Investigating the effective use of costly Operating Systems requiring proprietary platforms (e.g. AIX, HP-UX, Solaris) and migrate to less expensive open-source or standard platform systems;
- Analyzing the effective use of extraneous development and test systems and reduce or right-size the number of environments; and,
- Leveraging data tagging tools to appropriately classify data and assign correct data retention policies, overall ensuring effective and efficient cost management of storage.

Ongoing Operations

FY 2021 - 2031

HHS IT Infrastructure team will continue to work collaboratively with vendor partners and HHS IT teams in ensuring all systems are maintained and leveraging modern capabilities. Operational activities include:

- Technology Refresh: Perform ongoing review of hardware and software currency and develop refresh plans following industry-standard lifecycles;
- Vulnerability Management: HHS IT will ensure ongoing security controls through vulnerability scanning, reporting, and hardening of infrastructure systems.
- Asset Management: Leverage the BEP implementation of a single Asset and Configuration Management Database and perform ongoing review and validation of data; and
- Service Management: Leverage the BEP implementation of an integrated Incident Management, Change Management, and Problem Management system to ensure the use of best management practices related to service delivery.

Data Center Facilities Management

FY 2021 - 2031

HHS IT Infrastructure will continue to secure and maintain the operations of the data center. Through interagency and third-party vendor contracts, HHS IT Infrastructure will oversee the ongoing and routine maintenance activities of data center infrastructure, including backup power and generators, cooling units, and fire suppression systems.

Additionally, as migration to the cloud occurs over the next 10 Years, HHS IT Infrastructure will evaluate opportunities to further optimize the use of the Winters Data Center facilities by collapsing and consolidating extraneous server rooms, overall allowing for the repurpose of office floor space.

Resources Needed

HHS is a customer of DIR's Data Center Services program. This program is a managed services interagency agreement leveraging third-party service providers to provide infrastructure and support services, overall reducing the number of HHS

full-time employees. The cost of this managed service includes 24/7 operations and maintenance of computing located in two off-site peer data center facilities, server and mainframe infrastructure and support, operating system software and support, database system administration, vulnerability management, backup and recovery services, integrated service management, disaster recovery planning and exercise, 24/7 Service Desk, service catalog portal, chargeback financial management and reporting, and audit compliance assistance.

For servers that have received an exemption and/or maintained by HHS IT, the support operations must be conducted by HHS full-time employees, or other third party contracted personnel.

It is the goal and intent of HHS to leverage managed services, such as the DIR Data Center Services program, as much as possible to reduce the overall number of full-time employees of HHS.

Benefits to Texans

As HHS IT modernizes legacy infrastructure, there are direct benefits to the health and well-being of Texans. These benefits include improved responsiveness, improved availability of systems, and improved data security. For instance, the DSHS website utilizes cloud computing technology, which is easily scalable to meet performance needs. During the onset of the COVID-19 pandemic, there was a significant increase in the number of users accessing the DSHS website. By utilizing cloud computing technology, the HHS IT infrastructure support teams could assess the required additional capacity needs and add that capacity in minutes to the DSHS website. With that ability to add additional capacity, HHS IT was able to ensure that the citizens of Texas continued to receive important information, such as an interactive map of COVID-19 testing facilities, instructions for testing, and critical health and safety guidelines relating to the virus.

A continued investment in modernizing HHS IT Infrastructure is a critical element to the agency's overall efficiency and the delivery of critical services to clients. Utilizing a five-year life cycle refresh program with a staggered twenty percent replacement strategy will align with the state's biennial planning cycles and enable the most efficient use of legislatively appropriated funds and agency personnel. Everything the agency is able to provide is directly impacted by the efficacy of its IT infrastructure.

Security

Overview and Background

The HHS CISO manages the safety and protection of agency services and programs through the cyber protection of sensitive information and information resources. HHS maintains both sensitive, protected information and systems/applications that perform mission-critical functions for the state's safety net which require continuous security monitoring. Maintaining an optimal cybersecurity infrastructure and operations program reduces the likelihood of security breaches and helps protect confidential information from unauthorized access, use, disclosure, disruption, modification, or destruction.

Though guided by sound policy and supported by key legislative funding, these technology advances and the large number of HHS systems, networks, and devices increase the complexity, severity, and number of attempted breaches and potential for failure. While HHS IT has taken definitive actions during the past several years to improve its information security program, achieving compliance is a dynamic challenge across the complex HHS system. As we get smarter, cybersecurity perpetrators also get smarter. It is a cycle with no end, continuously challenging the agency's ability to protect its cyber environment.

As a result of HHS Transformation, HHS information security policies were updated to ensure security standards are consistent across all HHS agencies. One of the five lead IT divisions, the CISO maintains the HHS Information Security program. While CISO has made much progress, a robust security program requires conscientious attention and ongoing adjustment. During recent legislative sessions, the Texas Legislature has recognized the importance of cybersecurity, including by passing HB 8, 85th Legislature, Regular Session, 2017, and SB64, 86th Legislature, Regular Session, 2019. Funding was approved in the 86th Legislature, Regular Session, 2019 for HHS IT Security was dedicated to improving the agency's security posture, conducting a comprehensive security risk assessment of certain legacy functions, implementing software code scanning tools, and implementing a risk management plan to address vulnerabilities. Agency security processes developed this biennium for risk assessments and analysis of functions are repeatable across HHS in a risk-based approach to implement ongoing compliance with federal and state security requirements.

Technology has transformed the way HHS conducts daily business. Program staff depend on the reliable functioning of critical programs systems and infrastructure.

While modernization has added important capacity and capabilities, cybersecurity attackers also leverage the complexity of the systems to exploit system's infrastructure's weaknesses placing HHS's resources at risk. A specific example is HHS's rapidly evolving use of cloud computing services which has brought new and different risks to ensuring information security while also bringing multiple benefits like ease data access, flexible technology options, expanded storage as well as the elimination of needing to invest in and maintain dedicated hardware. The multiple threats to cloud computing services which can be met, if planned, developed, and implemented according to best practices.

However, even with state-wide focused efforts to achieve compliance and protect customers and agency functions, HHS faces a uniquely dynamic challenge among such a vast, complex system. All individuals with data stored by HHS systems, including Texas citizens' Personally Identifiable Information (PII) and PHI must be protected from data breaches or malicious acts. There has been a rampant growth in malicious software and attacks, with breaches in January 2019 being reported at nearly 2 billion records worldwide. It is estimated by Industry Security Leaders that the cost per hacked record is \$150 or higher. Texas and other states (i.e. Louisiana, New Mexico, Florida) have already been impacted.

The security threat to confidential information continues to grow and represents one of the most serious challenges that HHS agencies must confront. Security of HHS information depends on the ability to protect the agencies' critical systems and infrastructure in the face of such threats. Continued funding to address this constantly evolving environment is a mission critical necessity for HHS to remain vigilant in protecting the data of Texans and their access to key services.

Current State

HHS has prioritized information security by elevating the CISO to one of the five lead IT divisions. The CISO directs system-wide security policies, standards, controls, guidelines, and procedures to protect both HHSC and DSHS systems, networks, programs, and information. A key CISO component is the HHS Information Security program which maintains compliance with state and federal security requirements for protecting from digital breaches.

HHS Information Security program covers people, processes, and technology overseeing administrative and technical operations. It is based on well-established federal, state, and international frameworks, standards, and strives to implement and maintain industry best practices. To ensure staff is prepared, the Information Security Program has established the HHS Information Security/Cybersecurity

training to enhance the skills of security employees and to improve security awareness to counter different types of cyberattacks for all HHS staff. To improve HHS processes and decision-making, the Information Security program has implemented an enterprise approach to security leadership and governance for collaboration on risk reduction. To enhance HHS security measures, the Information Security program has employed new scanning tools to monitor technology while preventing and responding to threats and vulnerabilities.

The HHS Information Security program maintains five core functions to protect HHS agencies against cyberattacks: identify, protect, detect, respond, and recover. These five functions work together to create a cohesive system of protection.

- Identify: The program will assess, identify, and develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect: The program protects assets by continuing to review, develop, and implement appropriate safeguards to ensure delivery of critical services or contain the impact of a potential cybersecurity event. The key to comprehensive security protection is the ability of an organization to detect threats.
- Detect: The program develops and implements appropriate activities to quickly identify the occurrence of every cybersecurity event. Timely discovery of cybersecurity events is of utmost importance when seeking to contain the potential damage.
- Respond: HHS continuously develops and implements appropriate activities to take swift action in response a detected cybersecurity incident. The ability to contain the impact of a potential cybersecurity incident is key.
- Recover: The Information Security program continuously develops and implements appropriate activities to maintain plans for system resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

These five distinct yet interconnected functions work together to evaluate and detect potential cybersecurity risk to the agency, facilitate informed risk management decisions, address daily threats of security breaches, and improve future response by learning from previous activities. While definitive security improvements have been gained during the last several years, there are still priorities that need to be planned, budgeted, and executed. These functions are performed concurrently and continuously to create an agency culture that addresses constant, dynamic cybersecurity risk.

In addition to the overall functions of the HHS Information Security Program, there are three divisions to focus on the different aspects of HHS information security. The Enterprise Governance, Risk, and Compliance (GRC) platform⁶ seeks to ensure holistic management of information security issues. It is comprised of three main functions.

Governance

Security Governance addresses the policies, processes, and procedures in place to evaluate the security of processes, software, or hardware. This approach manages and monitors the organization's regulatory, legal, risk, environmental, and operational requirements to understand and inform the management of cybersecurity risk. Goals and objectives for Security Governance include:

- cybersecurity strategy and goals;
- standardized processes;
- enforcement and accountability;
- leadership oversight; and,
- resources.

While a highly protective HHS Security Plan with strong goals and objectives has been devised, consistent implementation and management of that plan across the agencies is key to its effectiveness. There must be a common understanding of security principles by staff and repeatable security processes by all divisions. Consistency is critical to ensure that the security management approach for reducing risks is applied throughout the organization.

Risk

Risk addresses establishing configuration baselines, execute security awareness campaigns to communicate best practices for security information to HHS staff, and training HHS staff to employ knowledge-based work habits and recognize the warning signs of a cybersecurity breach. The Risk team manages security risk for the agency and conducts analyses to examine the vulnerabilities associated with the system environment. The goal of these ongoing analyses is to develop and maintain a list of system vulnerabilities that could be exploited by the potential threat sources. Proactive methods, such as employing system testing, can be used

⁶ A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed. In personal computing, a platform is the basic hardware (computer) and software (operating system) on which software applications can be run.

to identify system vulnerabilities efficiently, depending on the criticality of the program and available resources.

Compliance

Compliance focuses on the need to conform with federal, state, and HHS requirements. State and federal policy and administrative rule require HHS to monitor its computer networks, ensure client privacy, and protect confidential information. These mandates include Texas Health & Safety Code, Texas Government Code, Texas Business & Commerce Code, TAC 202, Internal Revenue Service Publication 1075, Center for Medicare and Medicaid Services (CMS) policies, Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act, Family Educational Rights and Privacy Act (FERPA), and the Federal Information Security Management Act. Continued funding is necessary in order to ensure continued compliance with these multiple requirements.

Cybersecurity Operations Center

The second major component of the HHS Information Security Program is the Cybersecurity Operations Center (CSOC). The CSOC is a technical team with processes and technologies in place that monitor and respond to HHS security incidents and threats. The CSOC monitors security threats by assessing established security policy criteria, responds to security incidents by delivering a suite of cybersecurity response services, proposes architect security designs ensure successful integration within the enterprise environments, provides security services such as scanning, penetration testing, vulnerability and threat management and seeks data loss prevention by overseeing breach management processes and policies, information controls, secure communications, information rights, data classification and post-breach remediation, and security.

Potential Impacts of Threats & Risks to Critical Systems and Networks

In 2001, the Texas Legislature began to secure critical state infrastructure with the creation of the State Infrastructure Protection Advisory Committee. The committee was charged to review and make recommendations for protecting Texas' cyber environment. During the subsequent years, federal and state laws progressed to include cybersecurity as a required part of risk management. HHS sees cybersecurity as a key IT function and supports the CISO to protect HHS systems, networks, and programs from digital attacks. Similar to financial or legal risk,

cybersecurity risk has the potential to directly impact HHS's credibility and delivery of services.

Cyberattacks have increased dramatically over the last decade, exposing sensitive client and agency information, disrupting critical operations, and damaging the public's faith in government's ability to keep their information secure. Digital threats are rapidly evolving and the protection of the HHS system from attack, via a strong cybersecurity program, has become more important than ever. HHS' reputation as a healthcare provider is built on trust as we are responsible for protecting clients' sensitive personal health information.

It is well documented that security breaches (both malicious and human error) are real, costly, and time-consuming. Additionally, it is a violation of the public's trust. Citizens should not need to be concerned that their private information is discoverable through an internet search. Currently, the HHS Information Security Program is well positioned to continue progress as directed by statute and funded by the legislature. In order to maintain that position in a constantly evolving landscape, there are also additional strategies that need to be planned, budgeted, and executed.

Desired Outcome and Future State

Cyberattacks have increased since the onset of the COVID-19 pandemic, changing the entire threat landscape for cybersecurity. As the agency rapidly shifted to remote working, the HHS Information Security program continues to mature in protecting the confidentiality, integrity, and availability of agency's information systems. The success of cybersecurity operations for both HHSC and DSHS is contingent on the following:

- Access to comprehensive security training for HHS staff, and continuous communication and resources to ensure all are aware and vigilant against cybersecurity threats.
- HHS IT development processes will include expanded consideration of cybersecurity measures and participation of security staff, enhanced security roles and responsibilities for all HHS staff.
- Robust security monitoring via the Enterprise GRC platform allowing for the management of the lifecycle of agency policies, assessing and responding to risks, and reporting compliance with internal controls and regulatory requirements.

- Strong security management systems that enable detection of security incidents at an early stage and attempt to mitigate consequences before major damage is done. Future strategies include highly effective scanning and visibility tools that protect HHS against hackers, 3rd party security vulnerabilities, and malicious traffic that could compromise agency systems.
- Solid network security to improve the process for managing and authorizing access to HHS' data networks. Develop and implement a strategy to automate the ability to initiate, capture, record, and manage network user identities and access permissions to ensure the correct individual has access to the resources at the correct times for the correct reasons.
- Sustain the critical strength of CSOC to continue to quickly detect and respond to advanced threats. The reduction and/or elimination of ransomware and other potential threats against HHS translates to a reduction in the risk of associated costs from data breaches.

Timeline

The security modernization strategy seeks to build upon recent gains and to make strategic, incremental steps to identify and remediate security vulnerabilities and weaknesses to create a holistic, redundant security system. Security staff is continuously improving agency compliance with state and federal guidelines to maintain the most current security risk management information and/or guidance. Both HHSC and DSHS have ongoing projects (via the BOP and the Biennial Agency Security Plan) to enhance the current security infrastructure for the transmission and ongoing monitoring of data within HHS and its data trading partners.

During FY 2020-21, HHS was awarded \$35,856,054 to invest and address cybersecurity issues. Over the next ten years, HHS will need to invest consistently to ensure optimal cybersecurity. These funded improvements give HHSC application teams an important tool to use during development to identify and remediate security vulnerabilities and weaknesses before production.

Information system security plans and risk assessments include the on-going processes of discovering, correcting, and preventing security weaknesses. These include application assessments via application vulnerability scans. If potential application security weaknesses are not prevented or discovered and remediated, the risk of a potential data breach could occur. This could prove to be costly in both the potential fines associated with certain data breach types but in the loss of public trust.

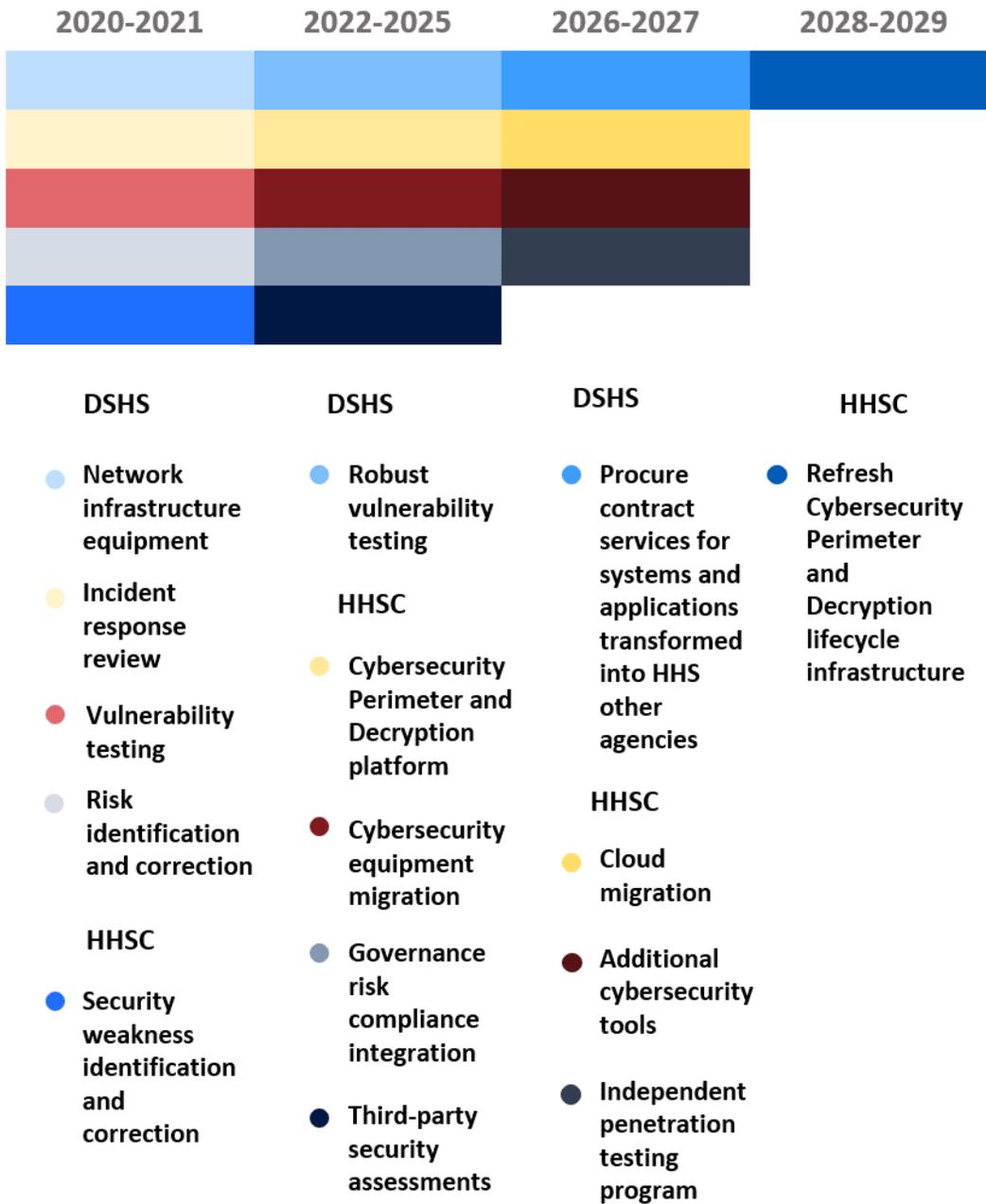


Figure 7 Security Timeline

FY 2020 - 2021

The DSHS network infrastructure equipment is being deployed and maintained based on new cybersecurity risks and necessary tools to combat the risks.

Vulnerability testing will be conducted, the results will be analyzed, and any identified risks will be remediated during FY 2021.

FY 2022 - 2023

DSHS seeks to build on continuous improvement, including advanced security monitoring and efforts to improve the agency's security posture. These efforts will be accomplished through the consolidation of security infrastructure and incident response processes within HHS, and improvements in risk identification through an expansion of vulnerability testing.

As part of a large security exceptional item (EI), HHSC has proposed a request for \$4.4 million as a subcomponent for the HHS Cybersecurity Perimeter and Decryption platform. This platform will allow for increased capability in detection and prevention, increase visibility into the agency's network traffic to allow improved security monitoring, and allow better strategies for managing potential risk.

FY 2024 - 2025

In FY 2024-25 it is estimated that the agency will request \$10.1 million for HHS Cybersecurity Security Information and Event Management migration, cybersecurity equipment migration, governance risk compliance integration, and conducting third-party security assessments. These efforts would ensure a secure architecture is considered and implemented, as well as the deployment of a cybersecurity platform to protect agency cloud infrastructure.

FY 2026 - 2027

To align with the HHS Information Technology and Data Services Modernization Plan, it is anticipated that the agency will request \$8.0 million to move business processes which are currently on-premise or located in managed data centers to cloud-based solutions. Additional cybersecurity tools will be needed for this key platform. This funding will also establish an independent penetration testing program to continuously improve the security posture and comply with the National Institute of Standards and Technology (NIST) requirements.

FY 2028 - 2029

It will be time to refresh the Cybersecurity Perimeter and Decryption life cycle infrastructure with an estimated cost of \$9.0 million. This effort will seek to maintain effective security in the most efficient manner with the least amount of

complexity while proactively reducing risk, meeting regulatory requirements, maintaining privacy, and supporting HHS system initiatives.

Over the entire 10-year period, a procurement of contract services will be needed for DSHS, DFPS, and systems and applications transformed into HHS from DADS to increase their security capabilities and continue to comply with safeguard requirements of HIPAA, TAC §202, Health and Human Services Circular C-021 and HHS Information Security Policies and Standards.

Benefits to Texans

There is no question that every day millions of Texans trust HHS with personal, financial, and other sensitive information requiring protection at the highest levels. Millions rely on the delivery of critical services for basic life needs or assistance to foster independence. Maintaining a mature, redundant cybersecurity infrastructure and operations program that incorporates best practices, reduces security attacks, and protects the critical services HHS provides is an endeavor the State of Texas should continuously support.

Legacy Systems Modernization

Overview and Background

HHS Application Services oversees the development, deployment, and ongoing management of the agency's software application suites. Application Services manages over 300 applications that support multiple stakeholder types. These stakeholders consist of: internal programs and departments within HHS, external stakeholders such as partner governmental/care agencies, and the citizens of the State of Texas that receive state supported benefits and care. These applications include some of the largest and most complex systems in Texas, including but not limited to:

- TIERS;
- MMIS;
- NEDSS;
- TxEVER;
- Client Assignment and Registration System – CARE;
- Clinical Management and Behavior Health Services – CMBHS; and,
- Centralized Accounting and Payroll/Personnel Systems (Financial and HR) – CAPPS-FIN and CAPPS-HR.

The Application Services division also provides support to all program areas of HHSC and DSHS. The supports that Application Services provides include:

- Support of multiple types of applications to provide HHS the flexibility to choose appropriate applications for HHS business partners and care providers. The application types fall into one of the following categories:
 - ▶ Internally developed applications – This application model requires specially skilled programming staff and a higher level of effort to maintain.
 - ◇ PROS: Can deliver exact functional requirements as specified.
 - ◇ CONS: Costly to deploy and maintain, require infrastructure, and have a longer time to market.
 - ▶ COTS applications – This application model requires deployment operational, and maintenance oversight.

- ◇ PROS: Industry best practices for business functionality, can reduce time to market;
 - ◇ CONS: Costly to deploy and maintain, require infrastructure and staff to run application.
- ▶ COTS applications modified with internal development – This application model requires programming staff, along with operation and maintenance oversight.
 - ◇ PROS: Provides industry best practices and is customizable to specific requirements;
 - ◇ CONS: Costly to deploy and maintain, require infrastructure, and have a longer time to market. Some vendors do not allow customers to own the core code base for these applications, which creates a complex relationship between customers and vendors. Many times, support contracts are limited to core code only, leaving all customization as the customer team’s responsibility.
- ▶ Software as a service (SaaS) applications – This application model requires oversight rather than maintenance.
 - ◇ PROS: Industry best practices for business functions, cost of development, infrastructure, and maintenance provided by vendor, several license models to manage software costs.
 - ◇ CONS: Many do not allow customizations, contracts for data ownership must be scrutinized, and many perform software updates only by the vendor’s schedule.
- Application Services also includes developers and programmers who write code for new and existing applications as well as system administrators who maintain production applications. Application Services is responsible for supporting applications through all phases of the software development lifecycle by:
 - ▶ developing applications;
 - ▶ writing code to enhance and maintain applications;
 - ▶ working with vendors who provide support and maintenance for applications;
 - ▶ testing applications;
 - ▶ keeping applications up and running;and,
 - ▶ deploying applications.

Current State

Inherited Applications

As a result of the HHS Transformation effort, Application Services inherited a number of applications from the transformed agencies. These legacy applications were brought under HHS IT's management, but were not initially reviewed for functionality, health, age, security vulnerabilities, or user communities. By accepting responsibility for all running applications from previous agencies, HHS IT was left with an inventory of applications with duplicative functions, poor states of health, security holes and vulnerabilities, and an age at which most developers with the skillset to maintain the applications are long retired. Additionally, the pre-Transformation agencies' software development lifecycle processes, operational processes, change and incident management policies, patch processes, and security processes all had different approaches that are still in use today. Tools to monitor and operate the applications vary widely as well. These inherited differences cause delays in general operational support and maintenance, make cross team support difficult, and create inconsistencies in matching applications to their corresponding infrastructure.

Disparate and old infrastructure produces another set of challenges. While some HHS applications are maintained within the DCS infrastructure model, others are not. Applications and infrastructure are also deployed outside DCS, such as the Riata Data Center and the HHS Winters Data Center. There are also a variety of non-HHS approved applications installed on desktops and laptops within cubicles of various HHS office buildings because past procurement processes allowed program areas to purchase applications without IT staff involvement. This de-centralized infrastructure model has led to complications in accurately cataloging where applications are stored, tracking application refresh cycles, and difficulty in backing up and recovering application data stored on desktops in office buildings. Disconnected applications and infrastructure are prime targets for security breaches and hacks, data loss and corruption, and wholesale application failure without any method of recovery. Without continued funding, departments are at risk of losing their data; provider partners are at risk of losing their processing ability, and the citizens of Texas are at risk of having their personally identifiable information compromised.

The HHS CTO led an application rationalization study to help HHS IT identify duplicative and outdated applications. The rationalization study is providing Applications Services the data they need to group applications by business

processes/capabilities and create a strategic approach to reach their desired outcome and future state.

Support Models

There are inconsistent support models for Application Services that do not align with best practices as outlined in the IT Infrastructure Library (ITIL)⁷ for Service Strategy, Design, Deployment, and Operations. Support varies by application portfolio⁸, and program-owned applications are often not supported by Application Services, which led to databases and applications being deployed with no long term operational or maintenance plan. For some applications, there are challenges with proactive monitoring. Application Services uses some outdated monitoring tools that carry the following risks for program-owned applications:

- A higher risk of security vulnerabilities and data corruption.
- Security patches do not get deployed, leaving these systems wide open for hacker attacks.
- With no database back-ups and maintenance, there is a high probability of data corruption, leakage, and loss.
- Exposure of HHS client's personally identifiable information.

Custom-Developed Applications

HHS runs many custom-developed applications that take longer to deploy and require internal human and technological resources to operate and maintain. These custom-developed applications have difficulty staying current with features/functionality, security updates, and operating patches as they require the services of the developers/programmers to rewrite and update code bases to keep the application working. Custom-developed applications sometimes do not provide the usability expected by HHS clients and partners.

Applications requiring a Mainframe System

Currently, HHS Application Services supports three legacy applications operating on outdated mainframe systems:

⁷ IT infrastructure library (ITIL): ITIL is a framework of best practices for delivering IT services. ITIL's systematic approach to IT service management can help businesses manage risk, strengthen customer relations, establish cost-effective practices, and build a stable IT environment that allows for growth, scale, and change.

⁸ Application Portfolio: an organization's collection of software applications and software-based services, which it uses to attain its goals or objectives.

- The TMHP MMIS is a group of applications that includes a mainframe component. This group of applications handles all Medicaid fee-for-service claims for the State of Texas.
- CARE - This is the central client database for the Mental Health and Intellectual or Developmental Disability (IDD) components of HHS. Some HHS entities that use CARE are state hospitals, Local Mental Health Authorities, and Local IDD Authorities. Care also manages 1915(c) waiver interest lists and plans of care for individuals with mental health issues and IDD.
- Intellectually Disabled Client Assignment and Registration System (IDD CARE)–This is another client database for clients with IDD that functions similarly to CARE.

HHS uses IBM Model 204 mainframe systems, which are large, physical, specialized computers that were developed by IBM as early as 1952. In the 1960s and 1970s these systems gained broad usage as they could process large amounts of transactional data and act as a database management system. Mainframe systems require specialized operating systems, programming languages, and system components to maintain. They served their purpose during the days of early computing but have since been replaced with more advanced database and web applications. The skills necessary to maintain mainframe systems exist with individuals at or past retirement age, and there is no new resource to replace them as universities no longer teach courses related to this field. Application Services is challenged to find vendors and state staff that can maintain these aging systems and applications, as well as replacement components when breakage occurs with these nearly 40-year-old systems. Mainframes present a higher security risk to HHS client data because they are incapable of meeting modern security standards. Because of their age and functionality, these mainframe systems make data collection for reporting difficult.

Staffing

Currently, Application Services is unable to take full advantage of current software services due to a lack of human talent resources. Many current Application Services staff members do not have training with ongoing software development and operational procedures. This lack of training means that HHS continues to use older technologies that become more difficult and costlier to support long-term. Programs and clients are impacted by being unable to take advantage of newer technologies that have played a role in improved services industry-wide.

Desired Outcome and Future State

The desired outcome of HHS IT system modernization relies heavily on the modernization of the HHS IT infrastructure. A modernized IT system requires modernized IT infrastructure to work optimally and deliver the benefits of increased productivity and reduced operating costs. Systems will have real-time automated monitoring of applications, backup services, and data. Moving to the cloud will also allow the Application Services division to be efficient in the delivery and operations of modernized application environments that provide the best service to Texans. An example of an efficiency gain of system modernization would be the secure around-the-clock functioning of the HHS IT Incident Management team. Another efficiency gain would be the ability to effectively utilize data from different applications to allow HHS to make the best-informed decisions for its clients.

Application Services is moving to an Agile application development process, which includes migrating up to 80 percent of all applications to the cloud (Infrastructure as a Service – IaaS), where possible. Moving infrastructure to the cloud (IaaS) provides the following benefits:

- The cost of deploying/maintaining infrastructure is transferred to a 3rd party.
- Remove the need of agency staff to house and maintain hardware.
- Improved/modernized infrastructure and technology advancements.
- Top-tier security and performance appliances.
- The use of modern backup systems and ample data storage will result in cost savings on archival storage needs.
- Real-time automated monitoring of applications.
- Provides the usability, functionality, security, and performance expected by HHS clients and partners.

Application Services is also implementing a Development/Operations (Dev/Ops) application operational model. Dev/Ops is a software operational model that combines software development, quality assurance, and service management operations into one unified process. This process offers operational advances such as:

- Faster time to implement new features.
- More efficient software testing and quality measures.
- The inclusion of core software developers in the organizational model for tiered support.

- Organizational agility and ability to react to changes in the environment.
- Development and deployment of applications in the timeframes expected by HHS clients and partners.

Upgrading to an enterprise-wide information technology services management (ITSM) system will give Application Services the advantages need to identify applications and their corresponding infrastructure.

This future state of HHS IT systems will be accomplished by:

- Creation of a single point of contact for programs, inquiries, and policy implementation to enable the program to plan and prioritize tasking.
- Having the ability to scale technical resources up and down to meet the runtime requirements of HHS business needs.
- Having the ability to hire and train skilled developers running open-source codebases that can easily be updated and maintained.
- Creation of a “build versus buy” decision matrix, consisting of no more than 10 questions, allowing for HHS to make the best decisions for the business needs of HHS and the public. This matrix will help prevent the agency from investing in custom software that could be easily sourced from the market with a lower cost of maintenance.
- The ability to buy COTS software and build custom software, where needed, for specific public health and human services business processes that can only be delivered by the State of Texas.
- Implementation and use of an Agile framework to develop, test, and deploy application features quickly. The use of an Agile framework will provide clients with quicker releases to production, less rework, and higher quality of deliverables in terms of meeting the business need.
- Implementation of a Dev/Ops pipeline.
- Ensuring applications are secure, scalable, and meet cross-functional needs for business processing and overall agency reporting.

Timeline



Figure 8 Applications Timeline

HHS Application Services' ability to modernize application suites and legacy systems requires multiple projects and programs. This modernization effort requires consistent management support, year over year funding, and constant review and adjustment as technologies continue to change. The timeline below is dependent on future funding availability.

Texas Vital Records

FY 2020 - 2021

- Increase secure access to Texas vital records for security of citizen personal data.

Production Applications Modernization

FY 2020 - 2021

- Development of the first custom cloud application on the System-Wide BEP will be a case management system for the Legal Services division. This application will be able to take advantage of all the technology advancements of the BEP (interactive monitoring, scalable compute power, active and archival storage, and data encryption features.)

Resources and Interdependences - FY 2020 - 2021

- Expansion of systems and infrastructure to the cloud to support additional services.

FY 2022 - 2023

- Work in conjunction with Data Center Services and Information Security to migrate production applications to middleware software and infrastructure that is reliable, scalable, and secure. Progress towards compliance and audit standards.
- Assess applications for duplicative functions; begin retirement planning; and continue building a full inventory of all applications and their underlying technologies in order to effectively provide operational support.
- The development and establishment of a "buy vs. build" decision matrix.
- Train, re-train, or hire developers to create applications with modern development technologies and tools.

Resources and Interdependences - FY 2022 - 2023

Critical to legacy application remediation is the process of completing an inventory of all systems, software, software tools, business owners, and other detailed information allowing an organization to adequately manage its applications portfolio. HHS will undertake this effort in order to define the direction for legacy system modernization.

FY 2024 - 2025

The full utilization of an information technology system management (ITSM) system will allow Application Services to use an integrated approach to ongoing application management. Disposition and modernization of all legacy applications begins to increase with a destination of:

- Retire all duplicative applications.
- Rewrite custom agency process applications on the BEP.
- Reinvest in customized COTS products that are needed for key business functions such as ERP.
- Replace standard business functions with COTS solutions.
- Replace standard business functions with SaaS solutions.
- Keep production applications in a healthy state.

Resources and Interdependences - FY 2024 - 2025

- The development and implementation of data governance and standards will enable data sharing and interoperability across applications. For clients, it could mean the difference between applying separately for multiple programs and providing the same data repeatedly versus providing the data once and having a system of referrals or exchanges in place to obtain additional services for HHS clients.

FY 2024 - 2031

- Applications begin the process of modernization. Migration of the modernized applications to the cloud continues until all applications identified for cloud adoption are migrated to their new environment.

Static Scanning of Code

FY 2020 - 2021

- Begin the implementation of static scanning of code subject to deployments to eliminate releasing code with security vulnerabilities.

FY 2022 - 2023

- Continue the implementation of static scanning of code subject to deployment for increased security; reduce/eliminate security vulnerabilities at time of deployment.

FY 2024 - 2031

- Static scanning of code is implemented, all code is now statically scanned before being deployed.

Agile Delivery Framework and Dev/Ops Pipelines

FY 2022 - 2023

- Begin the implementation of an Agile delivery framework.

FY 2024 - 2025

- A Dev/Ops pipeline is established and in use.
- Optimize the implementation of an Agile delivery framework.

Resources and Interdependences - FY 2022 - 2025

- The development and establishment of a Dev/Ops pipeline.
- Agile coaching and education for HHS IT and non-IT staff.

FY 2026 - 2031

- Operational efficiencies achieved through the modernization of systems and infrastructure allow a shift towards more application development.
- There are additional Dev/Ops capabilities and a mature Agile delivery framework in place.

Benefits to Texans

Investment in this area is essential for the long-term, ongoing effort to provide public health services in our state. The evolution of the HHS Application Services must be a priority for both the organization's management and legislative leaders for the State of Texas. These core applications are the information systems that maintain all the state's health data and benefits processing, including but not limited to; clients who receive benefits, such as WIC, SNAP, TANF, etc., reimbursement rates and history for Medicaid and Medicare funding, and personal information on citizens with infectious diseases, such as COVID-19 pandemic. The DSHS laboratory sciences systems include critical databases that contain the research information that run our public health programs; revenue from claims processing and payments are performed in the CARE applications; and Social Services Applications handle all benefit eligibility for the entire state.

Any security breach, loss/leakage of data, and/or unexpected disruption of service for any of these applications could lead to federal violations (such as the HIPAA Act), loss of state revenue (without partner/federal reimbursements), and overall brand destruction as millions of Texans' personal information could be at risk. During this time of a global pandemic, the HHS Application Services team is fighting to maintain these critical applications for the welfare for the citizens of Texas.

Data Services

Overview and Background

Over the past 10 years, the HHS system, legislators, and various stakeholder groups have identified a recurring need to enhance data governance and data management standards applied to HHS data and to develop and implement coordinated performance measurement and advanced data analytics tools that foster data-driven decision making.

In 2010, the HHSC conducted a needs assessment and alternatives analysis to identify an analytical system (Vision 21, Medicaid Fraud and Abuse Detection System (MFADS), or TIERS Data Mart) that could provide the member and provider-centric business intelligence capabilities identified by Medicaid Enterprise stakeholders. No single system was identified that would meet all the needs for HHS at the time, and no off-the-shelf option was available.

In response to this assessment, HHS initiated the Medicaid Enterprise Data Governance program (EDG) and began Enterprise Data Warehouse/Business Intelligence (EDW/BI) planning efforts. In 2014, HHSC submitted a request (Implementation Advance Planning Document (I-APD)) to the CMS to implement the Medicaid EDG program, which sought to create a framework that aligned data governance and data management across HHS along a series of Medicaid-focused initiatives.

In addition to recommending a number of structural and functional changes across HHS, the 2015 Sunset Advisory Commission Staff Report identified specific findings, deficiencies, and recommendations related to data and performance management. Specifically, the report identified the need for HHS to pursue a centralized and more robust approach to data and performance management.

While the 2010 needs assessment and Sunset recommendations provided useful insight into the HHS data analytic and performance landscape, the transformation and agency consolidation that resulted from the Sunset recommendations made it clear that further evaluation and assessment of system needs, capabilities, challenges and priorities was required before the most appropriate approach could be identified and implemented. The EDW/BI was subsequently canceled.

HHS established OP in response to the legislative direction of SB 200. OP provides performance management and data analytics support. This work includes the

development of an HHS-wide performance management and analytics system that will provide a transparent and robust perspective on system performance in the delivery of health and human services as well as robust cross-system analytics to support data-driven decision-making.

As HHS has worked to better understand the performance and data landscape that grew out of transformation, it has become apparent that the original vision of developing a singular technological solution that would attempt to meet all of HHS data needs is not likely to be the best approach. Since the EDW/BI project was cancelled in 2016, HHS has changed tack to pursue a more flexible approach. The goal with this new approach is to focus on coordinated incremental progress. Using Agile methodology, it will build a series of interoperable component parts that can be interconnected as needs and resources are identified. This approach allows for smaller scale testing or piloting solutions, to ensure that they work before making large scale investments. The result will be a system that is strategic and responsive, addressing higher need areas more quickly, and one that can evolve, adapt, and maximize returns in a rapidly changing technological environment.

Although EDW/BI was cancelled, EDG continues to be an integral part of both HHS performance management and analytics efforts, its MMIS modernization efforts and its strategic approach to link new systems as HHS modernizes its IT systems. These efforts have and will continue to enhance HHS' ability to identify clients receiving services and providers receiving payments across different siloed IT systems.

In 2018, HHSC expanded data governance goals beyond Medicaid and embarked on the planning of an HHS-wide performance management and analytics system (PMAS) of technologies and capabilities to guide the HHS system by providing broad and deep perspectives into overall system performance, increasing transparency, improving communication and coordination within the system, and aligning system activity with agency priorities. This started with performance focused design sprints conducted with all HHS divisions over a two-week period to document each division's current (as well as future desired state) performance measures, including technical requirements (e.g. source systems, data lags, timing, etc.).

In 2019, building on design sprint information, a pilot was launched to test and strengthen HHS capabilities to visualize performance management dashboards by depicting the achievement of critical targets and day-to-day business objectives of two divisions, RSD and HSCS, through key performance indicators (KPIs) illustrated by supporting performance measures. Early feedback on this approach has been positive and HHS has taken several key lessons away from the pilot. As resources are available, HHS could expand the approach into other related areas to test and

improve on HHS' ability to develop and visualize cross-division metrics. This pilot also highlighted the need for integrated system-wide data connectivity and analytics tool availability. As resources are available, HHS plans to fulfill that need using the above mentioned Agile approach. These connections will be prioritized based on their ability to provide high-value data connections and analytics that will inform program decisions and support enhanced performance management dashboards.

Current State

HHS data, performance and analytical landscape today is largely fragmented, relying on hundreds of separate business system applications that were developed at different points in time based on a business need with little thought given to any future data interoperability, data integration, or advanced analytics. Analytic tools and capabilities across the system vary widely in maturity and availability. The area that has seen the most improvement in data maturity and analytic capabilities is Medicaid; however, Medicaid data still remains largely siloed from the rest of HHS data, even where clients and programs intersect.

Over time, HHS has been able to make incremental improvements to the HHS data and performance landscape. Master Data and Metadata are available to HHS staff for use in analytics – repurposed from their original intended use for enabling interoperability in an EDW environment. For example, staff now have access to improved provider addresses that have been verified as mailable and geocoded to enable more accurate analysis on network adequacy. Staff also now have access to technical information in the metadata repository that allow them to more quickly understand and use new data sources and perform more robust analyses.

The Medicaid CHIP Data Analytics data platform, originally planned as a staging platform for EDW activities, has added analytic tools, including a Tableau server, and is being used to create reports and visualizations related to trends in Medicaid utilization, maps to examine the adequacy of provider networks, managed care contract compliance performance measures, and statistical analyses to detect anomalies in data reported by the health plans. More recently, the creation of an integrated database on the platform automates the data extraction from multiple sources of Medicaid data to reduce errors due to manual manipulation. Manual data preparation activities are reduced, and analysts are able to spend more of their time analyzing data, which results in an increase in response times for requests for data and information.

In addition, HHS has created an Advanced Analytics team within CADS whose goal is to discover and analyze other sources of HHS data and determine best practices for integrating data from across divisions to better understand our clients and their needs, and to guide policy decisions that will lead to improved outcomes. The data asset repository allows staff to search catalogued data assets and discover new data sources. The metadata repository allows staff to quickly learn how to use new data sources.

The performance management dashboards pilot within the RSD and HSCS divisions has proven the value of increasing visibility into program performance. The pilot has successfully translated the HHS mission and goals into a comprehensive set of objectives and outcomes, communicated performance and goals, and provided essential information to division and agency leadership.

As mentioned above, the current HHS technology setting with multiple analytics hardware environments and agency-specific applications has created many challenges, including:

- Siloed performance management, data analytics, and databases within HHS divisions, programs, and services tax resources, inhibit efficiency and productivity, and make data synthesis difficult.
 - ▶ For example, a request for Medicaid information often results in analysts querying and extracting data from multiple sources with no standardization of data elements and varying degrees of quality. Analysts spend approximately 70% of their time extracting and preparing data before an analysis of that data can even begin.
 - ▶ RSD has 15 systems that manage similar information due to previous agency consolidations, causing data field names to vary widely (e.g. inspections are also called surveys and accreditations). Staff manually review all variables to integrate the data correctly, which contributes to extended data processing times.
- Data attainability challenges and data lags are prevalent, preventing the availability of appropriately timed data and timely performance analysis, which in turn affects timely problem solving and decision-making.
 - ▶ Due to claims adjudications, Medicaid/CHIP utilization and expenditure data are not reliable for eight months after the date of service.
 - ▶ Managed Care Organizations (MCOs) do not have visibility into what services are provided to children enrolled in the School Health and Related Services, a federally funded program, as it is billed through a

system currently inaccessible by HHS, the billing methodology is different, and information requests are prohibited due to FERPA.

- HHS' wide variety of complex data assets are incompletely catalogued, and although HHS has an established, repeatable process for discovering and defining these assets, there are still many important HHS systems that lack critical business metadata.
 - ▶ A lack of documented metadata impedes interoperability, automation, and connection of disparate data sources. This complicates HHS' ability to produce reliable analytics both within and across divisions.
- Despite implementation of an HHS-wide Metadata Repository many systems within HHS lack business metadata, limiting the discoverability of appropriate data necessary for complete and accurate data products.
 - ▶ Metadata management is critical for ensuring data quality, consistency, and accuracy of data across various reporting systems. For example, when an address is contained in a data asset, it can be unclear if the address is a home, mailing, or business address.
- Technology debt is the total implied cost to refresh technology components such as PCs, servers, storage, operating systems, anti-virus tools, database, middleware applications, networks, network components, and patching from their current state to where they need to be and is a significant challenge.
 - ▶ For example, Windows Server, Salesforce, and Oracle databases have varied development and refresh cycles necessitating precise monitoring and oversight.
 - ▶ Additionally, data quality and metadata management processes are different in Salesforce-based systems and large MMIS components designed for highly-reliable, high-volume payment transactions.

In addition, like many large and diverse organizations, HHS faces the following technology challenges related to expanding data analytics to other programs:

- Legacy systems and supporting infrastructure that are aging and costly to maintain, requiring substantial resource spending.
 - ▶ The CARE system, a critical long-term care transaction system, is still running on mainframe technology from the 1980s. Newer tools available today are largely incompatible.
- Lack of a reference system architecture for HHS analytics and coordinated data governance results in a heavy reliance on manual data integration, *ad hoc* analytic solutions, and retrospective performance visualizations.

- ▶ Data fields (e.g. county codes) are described and defined differently across the system, creating challenges with automating and merging data from various systems. Data must be manually manipulated before any analyses are performed or visualizations are developed.
- ▶ Efficiently managing bed turnover and waitlist capacity is a challenge, as jail discharge and readmission data for forensic patients, which are 70 percent of HSCS facility admissions, is not integrated. Manual research is required to link patients based on arrest dates from counties.
- ▶ Medicaid needs better integration with CMBHS, the mental and behavioral health data mart, to establish coherent client histories and track patients as they utilize services through a variety of HHS programs.
- ▶ Most MCS services are delivered through MCOs, but MCO self-reported data, including quality, access, and financial data, is challenging to monitor due to high volume and inconsistent data standards.
- Data management processes are not mature enough to support complex data analytics processes, delaying response times and limiting analysis capabilities.
 - ▶ Member and provider identity resolution, reference data, and data quality mitigation are not embedded in IT system architecture processes and development, necessitating manual efforts in analytics and performance measurement.

Desired Outcome and Future State

As a response to the SB 200 requirement and Sunset Advisory Commission recommendation, over the next 10 years HHS seeks to develop and maintain effective performance management and data analytics structures that will:

- Create an environment of integrated data that will continually mine systems and information to collect, link, organize, and analyze program data, offering near term cost avoidance;
- Build upon the success of KPI visualizations and expand the process across the system, providing insight into the various aspects of program success;
- Develop performance management systems using data governance processes to facilitate data management with advanced analytics tools to effectively measure data at the program level;

- Ensure data are secure, transparent, accessible, reliable, and holistic in nature, thereby functioning as a trusted source, protecting confidential information, and providing connectivity and seamless interoperability;
- Establish stronger data stewardship processes to keep the data in good shape for performance analysis;
- Fully automate performance management and data analytics to increase the speed of obtaining reliable information, reduce the risk of human error, and unbind critical resources;
- Create client-centric service histories to improve client satisfaction, maximize services, and increase positive client outcomes;
- Monitor and evaluate service delivery to foster data-driven decisions and create an environment of continuous improvement; and,
- Implement a prioritized list of issues and enhancements to be regularly assessed for development into division-specific and cross-divisional improvement.

As a result, all HHS system data will be fully governed and seamlessly interoperable with performance tools and analytic capabilities that allow HHS divisions and programs to achieve advanced business analytics, operating at maximum efficiency with the ability to predict and prescribe outcomes for individuals utilizing services. Examples of future capabilities include:

- Cross-agency data sharing and system analytics integration to enable analysis and decision support across historically siloed data domains.
- The ability to understand and adjust cause-and-effect theories related to all major HHS business operations and programs.
- Enhanced analytical capabilities to:
 - ▶ Identify trends and interpret patterns;
 - ▶ Make predictions;
 - ▶ Gain insight into client outcomes; and,
 - ▶ Generate recommendations and drive change.

Expected Achievements and Positive Returns

Integrating HHS data across the system will have positive impacts both on client outcomes and program expenditures. Following is a sampling of analytic initiatives

HHSC is pursuing that showcase potential benefits of expanding analytic capabilities and developing an interoperable performance management and analytics system.

Neonatal Intensive Care Unit Expenditures:

- By enhancing the quality and connectivity of maternal and child health data sets related to postpartum depression, cervical cancer screening, well-baby checks, and other related measures and offering program staff access to advanced analytics tool to mine that data for valuable insights, PMAS will allow policy makers to develop and implement processes that raise these measures and ultimately result in better outcomes for vulnerable Texans and lower costs for taxpayers.
- In FY 2018, 15 percent of newborns whose delivery was paid for by Texas Medicaid required NICU services at a cost of \$809 million, or \$26,459 per client. PMAS will provide opportunities for examining historical information, creating statistical profiles, and ultimately enabling the use of tools for predicting when a pregnant woman is at risk for delivering an infant who will need NICU services. Preventing NICU utilization results in reduced costs for inpatient facilities, managed care organizations, Medicaid, and other HHS programs that provide services for impacted children who may have ongoing health complications throughout their lives.

Intellectual and Developmental Disabilities / Physically Disabled:

- HHSC provides a range of services to individuals with IDD and/or physical disabilities in Texas, including campus-based direct services and supports within the SSLCs. By enhancing the quality and connectivity of data sets for the different services we provide to individuals with disabilities and connecting to data from other systems, PMAS has the potential to reduce admissions, re-admissions, and lengths of stay in SSLCs, while improving outcomes for individuals and lowering costs for taxpayers.
- HHSC also offers numerous waiver programs that provide critical supports to Texans with IDD and/or physical disabilities that enable individuals to live in their home communities. PMAS could pull data from external systems such as criminal justice, housing, and local agencies, to provide a more holistic view of the client, improve service coordination, allow more targeted supports and services, anticipate needs, and increase transitions to community-based care, which is significantly less expensive than residential services.

Behavioral and Mental Health:

- Behavioral health conditions are associated with significant physical comorbidities, which can increase the cost of care and result in poor health outcomes. Individuals with mental illness are also more likely to develop chronic medical conditions and become physically debilitated earlier in life, increasing acute and long-term costs.
- In FY 2019, Texas Medicaid CHIP Services spent nearly \$823 million on acute care services for behavioral and mental health related diagnoses and an additional \$45 million on acute care services for substance use disorder diagnoses. Individuals with both mental and physical health conditions may receive services in fragmented systems of care with little to no coordination across providers, which can lead to poor quality of care and high costs. Better care coordination for this population has the potential to improve health outcomes and control spending, as well as reduce homelessness and criminal justice system encounters.

Facility Management:

- HHS System Support Services (SSS) is responsible for overseeing the infrastructure support functions of the HHS agencies, which includes providing emergency and risk management oversight and guidance across HHS. The bigger challenges SSS currently face are facility-related safety issues at the state, central, and regional offices. SSS has a growing need to systemize and analyze information in a more timely, automated manner from data sources that can provide real-time information. By connecting all appropriate data sources and applying analytical tools, SSS would have a greater ability to tie individuals to an asset or location when an incident occurs, thereby increasing reaction time to, and outcomes for, potentially life or death situations.
- Currently, considerable resources are expended in lease costs, with HHS building lease costs at approximately \$100 million per year. Providing SSS with location-identifying capabilities will improve people and asset location and space utilization decision-making by granting the ability to identify and illustrate precisely where space reductions are most feasible, leading to considerable dollar savings.

Cost Saving Benefits:

- Based upon the projected costs and the estimated benefits with the start of PMAS development activity, a positive return on investment (ROI) is projected to occur during the FY 2024-25 biennium with the ability to connect

data sources and track and measure cross-program outcomes throughout the continuum of care.

- Due to EDG, a positive ROI is projected to occur in parallel and post implementation of the PMAS development activity during the FY 2024-25 biennium.

Privacy & Security

Solution data security will embrace the security policies of the enterprise, participating agencies, individual Medicaid programs, specific supporting operational systems as well as state and federal security mandates and best practices.

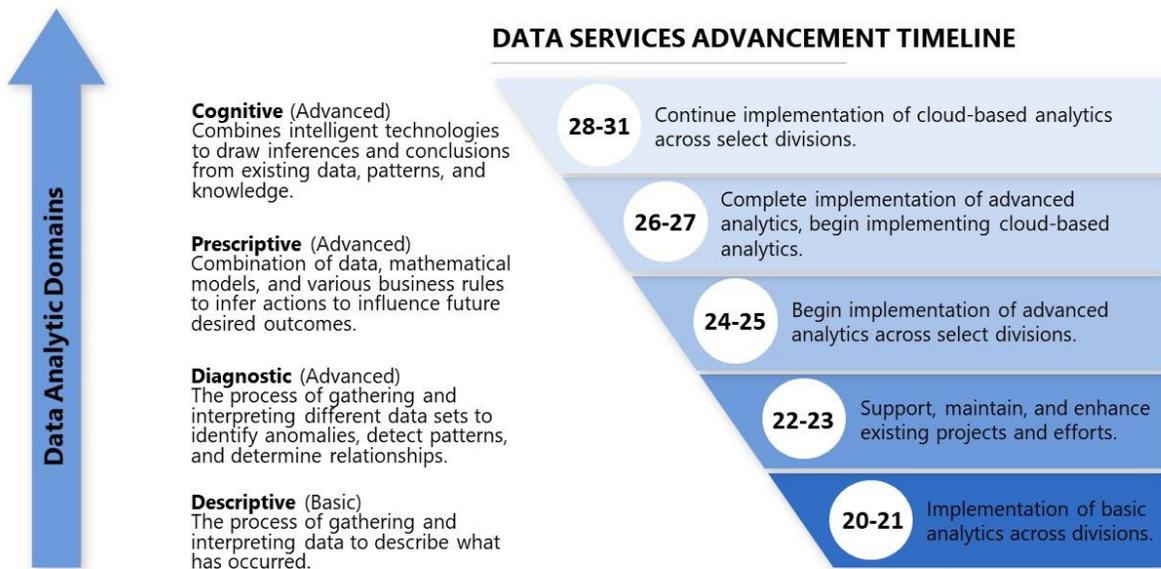
The information technology security framework used by HHS for security controls is derived from the Moderate-Impact system controls described in NIST Security and Privacy Controls for Federal Information Systems and Organization. Applying these controls would provide the security required for applications and/or systems designed to protect HHS from unauthorized access, use, modification, and destruction, and ensure the confidentiality, integrity, and security of PII and Sensitive Personal Information (SPI).

Timeline

HHS has a plan to achieve the desired future state with a solution that will be designed, developed, and deployed with an Agile/iterative approach. The approach is careful and methodical, and based on an agency wide needs assessment to ensure maximum benefit, proper ordering of legislative and agency priorities, and the ability to leverage and build on existing capabilities. With an Agile approach, HHS can prioritize and start benefitting from implemented capabilities sooner, improve outcomes for the people and entities we serve, and realize actual monetary benefits incrementally over time.

Analytics, or the analysis of data, can be described in two forms: basic and advanced. Basic analytics is characterized as descriptive, which includes operational reporting that is often manually completed, data exploration, and benchmarking. Advanced analytics can be characterized as diagnostic, which utilizes statistical analysis, predictive models, forecasting, and scenario planning to provide a better understanding of future scenarios; prescriptive, which improves the accuracy of predictions by continually processing and automating new data to fully optimize decision making; and cognitive, which involves machine learning and natural language processing, extending analytics to areas that were unreachable with more

classical analytics techniques like business intelligence, statistics, and operations research. Both forms of analytics will be implemented throughout the HHS system.



The strategy for achieving the desired outcome and future state will continue building on the successes already achieved and will be completed through an iterative process over each biennium.

FY 2020 - 2021

Using funding appropriated during the 2019 Legislative Session, HHS continues to develop, refine, and prove business value for piloted KPIs, and enhance the development of the Performance Management Dashboard (PMD) system, comprised of Tableau performance visualizations. Building KPIs within a division allows leadership to monitor activities, evaluate progress, detect problems earlier, and act before complications become irreparable. Additionally, KPIs give leadership the insight to discern when resources should be shifted, added, or reduced, improving business flexibility and management.

Recently, when the COVID-19 pandemic disrupted work and services in Texas as in other areas of the world, HHS was able to quickly put together a performance dashboard for the HHS COVID-19 response. This would not have been possible in such a short time period without the experience and expertise garnered from the PMAS KPI visualization pilot. For long term sustainability and successful system-

wide integration of advanced analytics and performance management practices, incorporating this in-house expertise within HHS divisions and programs is important in the future approach.

As Texas and the rest of the nation continues to respond to the COVID-19 pandemic, there has been increasing attention on the impact of the disease on different populations. HHSC is leveraging existing data analytics tools and resources within OP, and new tools developed as part of PMAS, to gather and analyze COVID-19 impact data from a variety of sources. This effort will occur in two phases:

Phase I:

- Phase I, which should be complete by November 2020, will involve the development of comparative dashboards for nine topical areas related to COVID-19's impact on vulnerable Texans, and publication of a relational/comparative analysis that examines potential relationships between as many of these topical areas as possible (e.g., attempting to evaluate COVID-19's mortality in a vulnerable population as it relates to that population's instances of testing, comorbidities, hospitalization rates, and complicating factors such as mental health diagnosis).

Phase II:

- Phase II, slated for Fall 2021, will involve a follow-up study that applies the initial research topics and any new questions gathered after release of Phase I to expanded data sets as they become available. In addition to providing more complete COVID-19 impact data, this plan will endeavor to explain trends, anomalies observed in the data and within the bounds of available data, and resources propose possible answers to the "why" questions raised by Phase I research.

HHS is also conducting a system-wide needs assessment to better understand each division's performance management, data management, and analytic needs, as well as identify data stewards familiar with strategically important datasets. Using information gathered, HHS will propose a technology roadmap that describes a methodical approach for deploying a data platform enabling integration of data and associated data analytic and performance capabilities across HHS.

A primary output for data governance processes at HHS in FY 2020-21 will be to develop and implement standards for data management policies and processes at HHS, guided by the DGPM ESC and DGPM Council.

FY 2022 - 2023

EI funding was requested to provide for one or two narrowly focused pilot projects; the Facility Management and the IDD / Disabilities projects described in the Expected Achievements and Positive Returns section of the Data Services chapter. These projects will provide opportunities to evaluate the benefits and return on investment associated with enhancing data connectivity across technology systems and applying analytics to those data sets.

Funding will also provide the PMD system with on-going support, maintenance, and enhancements required to implement additional operational measures, and continue proving the value of tracking key performance indicators. Data quality initiatives will also be initiated to improve data accuracy associated with PMD measures.

Additionally, these funds will contribute to continued support for the maintenance and enhancement of existing EDG efforts. Efforts include advancing master data management processes; data quality initiatives, collection, and enhancement of metadata stored in the HHS Metadata Repository for existing and new source systems; and maintaining the Data Asset Repository to remain in compliance with Sunset Issue 7 recommendations and the Medicaid Information Technology Architecture (MITA) initiative sponsored by CMS.

EI funding will also allow for the expansion of data stewardship roles to improve data management and data maturity initiatives beyond core Medicaid systems. This expansion, though limited, will further support the creation of an operational master data management system for the WIC program. Master data management would provide WIC the ability to identify Medicaid pregnant women and mothers that are not enrolled in the program and focus outreach and recruitment efforts on those populations. This could potentially bring an additional \$1,200,000 - \$1,800,000 annually to the state and HHSC due to increased WIC enrollment.

Based on the technological roadmap, data management roadmap, and the needs assessment, HHS will begin a procurement to implement performance management and analytic priorities. A data integration platform with an HHS-wide analytics data store will be procured using the new Texas State Data Center contract vehicle. This procurement will directly address and resolve the current challenges of siloed and program-specific analysis, data lags, and uncatalogued data assets. Additionally, this procurement will begin a feedback loop process across HHS programs that drive data-driven decision making, which will progressively mature with the implementation of the roadmap.

FY 2024 - 2025

Major HHS data assets that can contribute to master provider, client, and reference data will be available through the master data repository, a centralized, managed repository for highly-reliable identity and commonly used attributes. Governed data management processes will have been developed and implemented to de-duplicate, conform, and improve the quality of provider and client attributes. This capability will have created a shared, common collection of provider data for both individual and group providers. Published master data for clients, deduplicated and scored for quality, will be available for hub exchange or to serve API calls from other operational systems. Reference data adopted as HHS standards by governance processes will be available for analytic use, and to assist future alignment of IT operational systems as those are modified and replaced. HHS provider data, from Medicaid and non-Medicaid programs, will have been updated and managed to ensure accuracy of practice locations and contact data.

By FY 2025 the initial procurement of vendor services to design and implement a data analytics and performance measurement solution will be completed.

Analytics capabilities:

- Complete implementation of basic analytics for RSD; strengthening the division's capabilities to visualize performance metrics by depicting the achievement of critical targets and day-to-day business objectives.
- Begin implementation of artificial intelligence/advanced analytics for MCS, OIG, AES, IDD-BHS, OP, and HSCS.
 - MCS must have the ability to track dually eligible individuals (Medicare and Medicaid) to measure outcomes and identify cost and quality interventions when an individual is enrolled in more than one program, or their information is in multiple systems. If a client is dually eligible MCS does not have visibility into services provided by Medicare, or if the provider that is delivering those services is also a Medicaid provider. To gain insight, HHS must obtain data on dual eligible clients from Medicare and integrate the data with Medicaid client data.

Technical capabilities:

- Develop Tableau performance visualizations in HHS divisions and programs. While the PMAS pilot aimed at visualizing performance management dashboards in two divisions, the continuing effort will identify areas of opportunity for performance management and analytics within and across other HHS divisions. This effort will be followed by support and maintenance

of all visualizations including modifications and enhancements as well as automation of data acquisition, transformation, and deployment processes.

- Implement BEP integration.
- Data integration, data quality, data governance, and enterprise analytics.

FY 2026 - 2027

FY 2024-25 will see an expansion of the outcomes measures to the Chief Program and Services Office as a whole. At the same time there is a goal to enhance MCS and HSCS outcomes with algorithms and prescriptive analytics.

Analytics capabilities:

- Begin implementation of artificial intelligence/advanced analytic capabilities for RSD.
- Complete implementation of artificial intelligence/advanced analytics capabilities and begin implementation of cloud-based analytics for MCS, OIG, AES, IDD-BHS, OP, HSCS, and DSHS and Public Health data for infectious disease and bioinformatics.
 - ▶ The value of a fully cloud-based shared application development environment includes: Centralized data management with business intelligence, analytics, and artificial intelligence; faster time for new solutions; increased measurability, operability, efficiency & security; and elimination of legacy infrastructure and applications thus achieving smaller innovative infrastructure footprint.

Technical capabilities:

- Text: The process of converting unstructured text data into meaningful data for analysis, to measure customer opinions, product reviews, feedback, to provide search facility, sentiment analysis, and entity modeling to support fact-based decision making.
- Mobile: Mobile analytics captures data from mobile app, website, and web app visitors to identify unique users, track their journeys, record their behavior, and report on the app's performance.
 - ▶ HHS could enhance data captured from two public-facing mobile applications, "YourTexasBenefits" and the "Texas Veterans App."
- Social: The collection and analysis of statistical, digital data on how users interface with an organization, particularly online. Over the last decade,

social analytics has become a primary form of business intelligence used to identify, predict, and respond to consumer behavior.

- Location: Allows you to shape an in-depth view of your customers through combined data from your Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Electronic Commerce (eCommerce) online store and mobile apps, providing a means to reach customers with messages that foster a deeper emotional relationship with your brand.
 - ▶ Medicaid waiver bed locations could be graphed alongside state facility regions, so client caregivers can choose home care based on their location in proximity to service.
 - ▶ Currently overdose data is available, however data on overdose hotspots and overdose reversals is higher quality, but more challenging to acquire. Obtaining Emergency Medical Services (EMS) data and outside data sources would improve our ability to identify opportunities for intervention and alert communities of hotspots based on real-time data, allowing overdose reversals to be administered to a greater number of at-risk individuals at the right time.
- Graph (Network): An emerging form of data analysis, one that works particularly well with complex relationships. It involves moving data points and relationships between data points into a graph format (also known as nodes and links, or vertices and edges).
 - ▶ Virus outbreak concentrations can be graphed by county and superimposed on contact tracing and links to testing centers, providing critical information to healthcare providers.
 - ▶ HHS could benefit from the analysis of the numerous women's health programs and services offered by monitoring the data points (i.e., adolescents and women of child bearing age) as they progress through various, related services, allowing HHS to foster positive outcomes for clients and provide cost savings.
 - ▶ HSCS and IDD-BHS need patient matching across providers and transitions through many different systems to ensure follow up care is completed, potentially reducing adverse events and readmissions, and improving client outcomes.
- Imaged analytics: Categorizes images from social media and sorts them according to everything applied to text: gender, age, facial expressions, objects, actions, scenes, topics, sentiment, and brand logos.

- ▶ Machine learning algorithms can detect illness in Nursing Facilities or Women’s Centers from chest x-rays with accuracy exceeding practicing radiologists.

FY 2028 - 2029

Analytics capabilities:

- Complete implementation of artificial intelligence/advanced analytics capabilities and begin implementation of cloud-based analytics for RSD.
- Continue implementation of cloud-based analytics for MCS, OIG, AES, IDD-BHS, OP, HSCS, and DSHS and Public Health data.

Technical capabilities:

- Self-service reporting, Business Intelligence, data marts, and visualization.
- Client, provider, facility, and carrier (MCO health plans) 360 data marts.

FY 2030 - 2031

Analytics capabilities:

- Continue implementation of cloud-based analytics for RSD.
- Begin implementation of a feedback loop across HHS programs, starting with integrating basic analytics with advanced analytics, allowing analyzing data via complex algorithms, predictive analytics, and machine learning to guide data-driven decision making.
- Ability for users to merge HHS data with external data for ad hoc analyses as needed.

Technical capabilities:

Program area needs and technological capabilities will change significantly over time. In the last two years alone, advanced data analytics capabilities have evolved dramatically. PMAS will need to be able to evolve with program area needs and advancements in data technologies and this will have to be achieved through an agile approach to reacting to future technology capabilities.

Automation throughout HHS will have positive impacts across the system, which will translate to increased efficiencies, leading to more effective and cost-efficient services provided to HHS clients. Examples of these include:

- The use of image classification and advanced search capabilities, algorithms could filter the intent of records requests and provide available records without manual, administrative processes, or, at a minimum, would automate standard and typical requests.
- The use of predictive modeling and deep learning capabilities can identify trends that would not otherwise be apparent, even with descriptive data analytics, providing insight to cause-and-effect relationships.
- As fraudulent actors become more sophisticated, so too must the technology that identifies fraud, waste, and abuse. Integration of datasets, alongside 'human-in-the-loop' feedback algorithms (a model that requires human interaction) and similar capabilities will be required.
- Monitoring access patterns of users to protected data and automating the process of identifying and resolving alerts will require advanced data capabilities, and provide a secure, compliant, and protected data environment.
- Advanced analytic capabilities with 360-degree data integration would provide insight into client risks, allowing service providers to make necessary adjustments or actions to mitigate risk and potentially prevent the occurrence, overall improving client outcomes.
- Manual review processes of MCO submitted data are prohibitive, and automated analysis with algorithms would help MCS program areas identify actual concerns, while limiting redundant manual review processes that yield few results.

Other business operations that may be automated through relevant analytics capabilities include contract management and oversight, financial reconciliation, automated reporting, automated data quality monitoring and reconciliation, automated management of enterprise IT infrastructure, and automated customer service and issue resolution.

FY 2032-2033 (Exceeding the 10-year Plan)

Complete implementation of feedback loops across HHS programs. Enable a centralized team of dedicated, division-aligned analysts to provide ongoing support to HHS programs. As independent observers, the analysts are facilitators for change and provide direction, guidance, and assistance to programs in various aspects of performance management, analysis, monitoring and reporting. Ensure continuous improvement by conducting periodic reviews of business outcomes, evaluating impact of efforts on agency objectives, and measuring the achievement of outcomes and other quantitative and qualitative benefits.

Resources Needed

To reach the desired future state, HHS requires applied technologies that enable automation and machine-learning processes that can complement human decision-making functions, and well-managed data assets whose data quality is measured and managed.

To accomplish the objectives, 12 fulltime equivalents (FTEs)/contractors have been requested for FY 2022-23.

- CADS Staff: 10 FTEs
 - ▶ 2 of which will be allocated to specific data management areas.
 - ▶ 8 will focus on EDG related activities
- Information Technology Staff: 2 contractors

To achieve the objectives outlined in FY 2024-33, additional FTEs/contractors will be requested to support successful initiatives and fully realize the potential benefits of effective performance management and data analytics structures.

Investing in these resources is critical to the success of HHS' data analytics, performance management, and data management strategies. Doing so will support data-driven decision making, increasing HHS' ability to improve the health, safety, and well-being of Texans.

Identity and Access Management

Overview and Background

Identity and access management is the use of business processes, policies, and technologies to manage electronic or digital identities. IT managers use identity and access management to control user access to an organization's critical information.

Identity and access management is also an enterprise security tool used for cost savings and cost avoidance. The two primary methods that accomplish those are ensuring data security and providing a streamlined and consistent process of managing user access.

In 2019 the average total cost of a data breach across all industry sectors in the United States was \$8.19 million, with an average cost of \$150 per stolen record.⁹ With 77 percent of data breaches involving an insider, it is necessary to ensure access to all resources is secured and granted using least privilege access principles.

The HHS IT Identity and Access Management (IAM) division provides network and application access for over 80,000 users, which include: HHS employees, contractors, vendors, business partners, bidders, other state agencies, and over 300,000 citizen accounts.

IAM works to ensure that HHS staff and partners have access to the necessary applications and information that is required for them to serve HHS clients. When a user seeks to access any system or resource, he or she first enters the username as the very first step of identity verification into the system. The system then verifies the user's identity via the authentication process. Once the system completes the authentication process, the identity and access management system initiates the authorization process. This process ensures that a logged-in user is only allowed to perform the tasks which he or she is entitled to do as part of their job function based on the pre-defined security policies in the identity and access management system.

⁹ 107 Must Know Data Breach Statistics for 2020 Cost of a Data Breach Report
<https://www.varonis.com/blog/data-breach-statistics/>

IAM provides periodic reviews of access to ensure regulatory compliance. The objective of IAM is to provide automatic lifecycle management¹⁰ of identities and provision access to HHS applications and network resources. One service managed by IAM is the HHS Enterprise Portal. The Enterprise Portal manages access to 80 applications, 38 of which are deemed "mission-critical" for HHS. Some of the more familiar applications are listed below with their primary function:

ASOIG – Automated System of the Office of Inspector General.

ASOIG provides tracking, monitoring, and reporting capabilities on all overpayment and fraud referrals received into the system through various input methods. It generates an online statistical summary, detailed, and ad hoc reports. It provides the ability to establish, update, and perform an inquiry on clients' receivable claims using a real-time Accounts Receivable Tracking System interface. ASOIG contains the federally mandated Income and Eligibility Verification System match reports for both Texas Works and long-term care clients.

CAPPS Financials

CAPPS Financials is the HHS accounting and procurement system of record for the HHS system. This system is responsible for financial and procurement related transaction processing that occurs for the entire HHS system and is used to record core financial transactions.

IRIS – Integrated Resident Information System

IRIS is the Electronic Life Record used by the SSLCs. It provides a comprehensive view of the patient's diagnosis, medication, nursing notes, and therapies.

SWI – Statewide Intake

SWI is the Enterprise portal application used by DFPS Statewide Intake division to record allegations of abuse, neglect, and exploitation in the state.

¹⁰ Lifecycle Management: a collection of technologies and business processes used in creating, managing, coordinating, and restricting the identification, access, and governance of identities for access to business tools and information.

Automated Provisioning and Workflow

Automated provisioning is the ability to manage access to IT resources by using pre-defined procedures based on business logic that is carried out electronically through workflows without requiring human intervention. User accounts are automatically created, modified, or disabled based on inputs from authoritative data sources.

The automation of provisioning and access management can present a return on investment. True cost savings result mainly from the implementation of automated provisioning workflows and self-service tools that reduce the resources and staff required to administer access to an agency's information systems manually.

HHS Directory Services

The HHS IT Directory Services' main objective is to ensure the security of the HHS systems and networks by administering and managing HHS employee access to applications, systems, and information through Microsoft hardware and software platforms. Directory Services provides the hardware and software infrastructure support for identity and access management. For example, when a user logs into a computer that is part of a Windows domain¹¹, the directory checks the submitted password and determines whether the user is a system administrator or regular user.

Current State

HHS Enterprise Portal

The HHS Enterprise Portal is an interface that provides a single access point for HHS applications integrated with IBM's identity management platform. This interface is a secure platform where users and supervisors can manage access to integrated automated provisioned applications and integrated manually provisioned applications. The Enterprise Portal complies with HHS, the State of Texas, and federal security controls for access management and data security.

IAM manages access to 80 applications integrated with the Enterprise Portal, with automated lifecycle management for 53 of the 80 applications occurring in the portal. Users are required to manually request access to the remaining 27 applications through the Enterprise Portal. When an individual requests access to

¹¹ A domain is a network of computers, users, printers, and other aspects of security that are connected to a centralized database. A user at a client computer can log in to a domain to access resources made available to that user in the domain.

one of these 27 applications, it creates a task for the IAM Provisioning team to complete the request.

Access to the HHS Enterprise Portal and the applications integrated within it are dependent upon many external factors, including the HHS network, data center networks and components, application server health and connections, and more. IAM is currently unable to monitor potential problems that may occur among these dependencies. The inability to monitor or control for these potential problems presents a single point of failure, which results in a more reactionary than a responsive approach by IAM.

The Enterprise Portal also relies on hundreds of inner agency network connections between the hundred-plus servers that make up the Enterprise Portal framework and application team's servers for managing identity and access to HHS applications. The Enterprise Portal footprint spans across two state-owned data centers located in San Angelo and Austin. To mitigate the risk of loss of access, the IAM team has designed the infrastructure of the Enterprise Portal to have redundant failover¹². Having data centers distributed across Texas allows the Enterprise Portal to remain fully functional and operate out of either location in case of a disaster. This commodity comes at a steep price as it requires duplicate hardware; however, with the criticality of applications whose access is managed by the Enterprise Portal, it has been designed to be as reliable and resilient as possible within the technical limitations of the environment that houses it.

Identity and Access Management Outside of the HHS Enterprise Portal

The IAM Provisioning team manually provisions access for 58 applications not integrated with the Enterprise Portal. This manual provisioning is in addition to the 27 integrated applications that also require manual intervention to complete the access management process. The IAM Network Access Administrative (NAA) team provisions access for shared resources, including mailboxes, storage drives, and calendars. They also provide resources such as virtual private network (VPN) access, agency email distribution lists, and privileged accounts to HHSC/DSHS servers. The NAA team resolves over 50,000 requests annually.

There are hundreds of HHSC and DSHS applications whose access is managed outside of IAM; for these applications, it is the application owner's responsibility to manage access, remain in compliance with information security controls, and

¹²Failover: a method of protecting computer systems from failure, in which standby equipment automatically takes over when the main system fails.

resolve any audits as a resolute of non-compliance. The Enterprise Portal provides an automated option for application/system access to be managed by IAM; however, with the current antiquated IBM platform, the process of integrating new applications into the Enterprise Portal requires a significant amount of custom coding. It can take up to three months with current resources to fully integrate a new application and provide single-sign-on and automated access management functions. The current infrastructure is also limited in the amount of traffic it can manage. The ability for IAM to manage all system/application access for the agency is something the division strives to obtain over time, with adequate resources.

Desired Outcome and Future State

Identity and Access Management

Moving HHS Enterprise Portal infrastructure to a cloud computing model is based on industry best practices. A cloud-based or SaaS solution will provide IAM with the greatest amount of flexibility and scalability for expansion. A cloud-based solution offers high availability and will significantly reduce the amount of downtime customers experience in a given year, allowing them to be more productive and give clients better service. Another benefit of a cloud-based solution is powerful monitoring tools that will enable IAM to take a responsive approach to mitigate potential issues as opposed to the current reactive approach. This proactive approach will reduce disruption and ensure smooth service delivery of HHS applications to users and clients.

A cloud-based identity and access management solution using modern systems is flexible and capable of quickly expanding and contracting resources as business requirements change. This cloud-based solution will provide secure access to the applications that HHS staff and the clients we serve need at any time and on any device. It would enable the IAM team to integrate current HHSC and DSHS applications faster and improve the reliability of application access. With a highly configurable cloud platform and the scalability of cloud-based environments, access to all HHSC and DSHS applications would become centrally supported by the Identity and Access Management Team. This centralized support would improve agency security and add to the efficiency of agency resources by allowing access management functions to be automated.

With the new Enterprise Portal housed in the cloud, the environment goes from a binary to a tertiary environment, significantly increasing the availability for users.

The current uptime expectations for a Tier 2 data center is 99.9 percent uptime¹³, allowing for a total of 9 hours of downtime annually to be acceptable. A cloud environment is capable of increasing this up time to 99.99 percent or even 99.995 percent, which is the equivalent of 53 to 26 minutes respectfully of downtime annually. A cloud environment also removes the management of software and operating systems as the provider manages these.

Directory Services

Directory Services' goal is to consolidate and/or collapse the current Active Directory¹⁴ (AD) environment and infrastructure to use cloud-based technology to support the future infrastructure of HHSC.

Currently, the creation of a domain requires a minimum of two servers for domain controllers. The creation of a new directory infrastructure using modern domain services and minimal onsite support will allow domains to be managed on already existing infrastructure and eliminate the need for more servers and resources. Using existing domains will improve overall performance by taking loads off the network. HHS staff will have faster access to their accounts, in turn, allowing HHS staff to provide more efficient client services.

¹³ Data Center Uptime is annual guaranteed availability of a data center.

¹⁴ An Active Directory allows network administrators to create and manage domains, users, and objects within a network.

Timeline

The basis of the resource requirements for moving the Enterprise Portal was a review of the existing portal, integration code, and systems within the Enterprise portal. This review tallied the total number of staff hours required for the replacement of each system and the resources necessary to meet the proposed timelines for implementation.

Note: HHS IT Identity and Access Management's ability to follow this timeline is dependent on the availability of future funding.

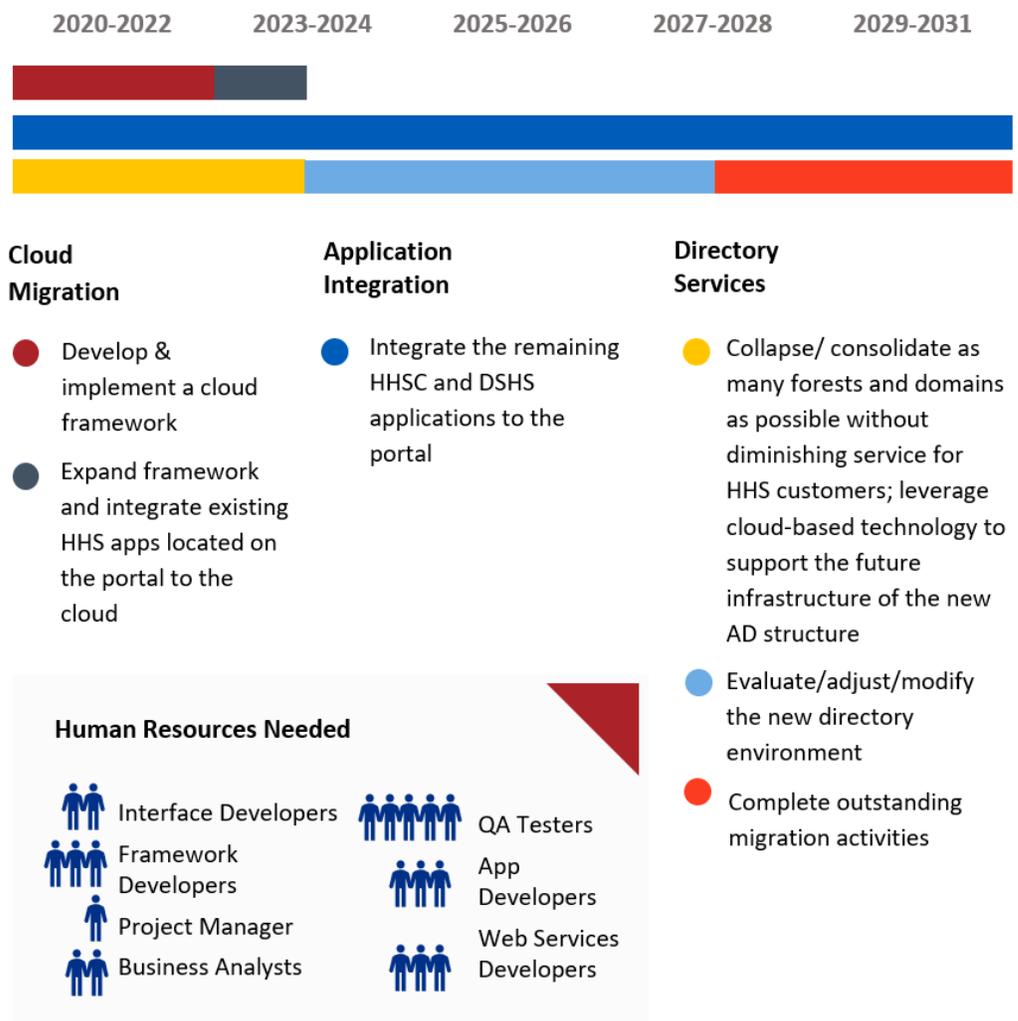


Figure 8 Timeline: Identity & Access Management

Identity and Access Management

FY 2020 - 2021

Work with the HHSC CTO office to develop and implement a cloud framework that supports the needs of IAM as part of the BEP project.

FY 2022 - 23

Expand on the IAM cloud framework provided and coordinate with application owners to begin integrating HHS applications to the new IAM platform (i.e., the Enterprise Portal).

HHS IAM will need the following contracted positions for the design, build and implementation of the cloud-based identity and access management solution:

Note: Contractors will augment to full-time equivalent employees to ensure timely migration of applications.

Resources FY 2022-2023

- One cloud architect to design the cloud platform.
- Two user-interface developers to rewrite the user interface.
- Three framework developers to rewrite the application framework.
- One project manager to keep the project on budget, on schedule, and within scope.
- Two business analysts to work with application teams and design application user interface.
- Five quality assurance staff, one lead, four staff to test/validate development work satisfy project scope.
- Three application developers to write code for the new IAM cloud solution to; programmatically identify users, determine if the user is allowed access, and transparently present applications to users.
- Three web service developers to write interface code for use between the IAM cloud-based solution and external applications. This interface coding is used by external applications to connect with the IAM cloud-based solution, ensuring that the application can integrate with the IAM solution.

FY 2024 - 2031

IAM will continue to integrate the remaining HHSC and DSHS applications with the HHS Enterprise Portal platform to have all identity and access management functions provided by the IAM team.

Resources FY 2024-2031

HHS IAM will need the following full-time equivalent employees that will either transition or replace contractors to continue with integration:

- Two user interface developer;
- One project manager;
- Two business analysts;
- Three quality assurance staff;
- Five application developers; and,
- One web service developer.

Directory Services

FY 2022 - 2023

Collapse and/or consolidate as many environments and domains as possible without diminishing service for HHS customers and to leverage cloud-based technology to support the future infrastructure of the new AD structure.

Resources Needed FY 2022 - 2023

In addition to existing staff, Directory Services needs third-party vendor services to assist in the environment/domain collapse and/or migration for FY 2020-21. Third-party services may be necessary to provide subject matter expertise in moving the agency to a consolidated AD infrastructure. Those services may evaluate and make recommendations for implementing a hybrid AD to support the agency's goals and state-mandated cloud offerings.

FY 2024 - 2027

Evaluate the new directory environment and adjust and modify it as required. As the agency's needs continue to change for applications, databases, rights and

permissions, and expansion into new sites, AD and AD Services will need to be modified to meet the needs. By evaluating and adjusting our services for business needs, we are ensuring continual service improvement to meet the needs of HHS and improve the delivery of services to Texans.

FY 2028 - 2031

Complete outstanding migration activities.

Benefits to Texans

The realization of the IAM and Directory Services' ten-year plan will benefit clients by providing HHS staff with a centralized platform for accessing applications, protecting client data by expanding the capabilities of the Enterprise Portal. It will ensure that all access complies with HHS security controls and that client data is protected against inappropriate internal and external access. With the ability to increase the number of integrated applications with automated access control, IAM will enhance the ability of the agency to protect client data and system access to a greater number of applications across the HHS system.

Converged Services

Overview and Background

HHS Converged Services oversees the agency's telecommunications and network infrastructure. The primary objective of HHS Converged Services is to provide a secure, scalable, and reliable enterprise-level network that provides voice, video, and data service delivery in support of the HHS programs charged with improving the health, safety, and well-being of Texans.

HHS Converged Services provides network services to more than 750 locations across Texas - including 24/7 support to 50 "critical service" locations such as SSLCs and state hospitals - as well as voice services to approximately 465 of these locations. Examples of services provided include: private multi-protocol label switching (MPLS) transport; establishment of the appropriate network type WAN, Local Area Network (LAN), or Wireless Local Area Network (WLAN)]; access to public and private cloud service platforms (e.g., Microsoft Office 365 (Office 365)) and DIR DCS; Internet access; unification and integration of communication modes and platforms; a physical client support center with remote support capabilities, for HHS telework and mobility initiatives.

HHS Converged Services must continue to acquire additional capacity to ensure the viability of existing infrastructure, which provides the support required to meet the evolving needs of the HHS program areas that oversee the delivery of client services. These ongoing efforts are also an essential component in HHS' business operations priority to expand telework and alternative work capabilities, particularly in light of the challenges that surfaced as a result of the COVID-19 pandemic that was declared a statewide public health disaster by Governor Greg Abbott. The COVID-19 pandemic necessitated HHSC Converged Services needing to rapidly scale capacity to handle support in excess of 30,000 new teleworkers, including 20,000 of which required secure VPN connections. These critical network services allowed remotely working HHS staff to continue delivering important services to Texans in need, while complying with shelter-at-home orders. Natural disasters, such as Hurricane Harvey, further illustrate the need for a resilient and scalable network that is able to reliably and continuously deliver services to Texans as the most critical times.

Regardless of whether demands on network capacity are temporary spikes due to events like those described above, or those in line with normal operations serving a

growing population, successfully meeting challenges on demand will require consistent integration of the latest technology, continuous improvement in network performance, and increased capacity.

All HHS programs depend on the HHS Converged Services infrastructure for service delivery. There are hundreds of HHS applications traversing the network that rely on a stable, operational network to ensure efficacious programs and benefits, most of which are mandated by state and federal laws, regulations, policies, standards, and guidelines are available to those in need. Beyond the obvious consequences of service delivery failure to HHS clients, such failure could also equate to non-compliance with federal mandates, thereby jeopardizing crucial funding upon which the system relies.

HHS System Dependencies

HHS oversees and administers a broad array of programs, all of which have varying levels of reliance on IT network infrastructure for secure and stable access to applications, cloud services, and remote teleworker functionality. Some of the most medically fragile and historically underserved populations in Texas rely on the following programs and services supported by the HHS Converged Services infrastructure:

- Medicaid for families and children;
- Disability Determination Services;
- Long-term care facilities for the elderly and/or those with disabilities;
- SNAP and TANF benefits;
- Chronic and infectious disease diagnosis, prevention, treatment, and laboratory testing;
- Newborn critical disease and disorder screening;
- Behavioral health services;
- Licensing and credentialing of long-term care facilities;
- Child-Care Licensing;
- Daily operations of SSLCs and state hospitals;
- Women’s health services;
- OIG;
- WIC;
- Vital statistics, including birth and death records; and,

- DSHS Epidemiology and Disease Surveillance Unit.

Current State and Risks of Network Infrastructure Failure

By the end of FY 2021, 48 percent of the existing HHS network infrastructure hardware and software will have reached manufacturer end of support, with that percentage exceeding 90 percent by the end of 2023. IT industry nomenclature refers to this juncture in a product's life expectancy as the End-of-Service Life (EOSL).

In addition to EOSL equipment no longer being supported by the manufacturer, repairs or replacements are often unavailable, and unavailability of security patches increases overall network vulnerability. Maintaining threat protection updates is an important component of protecting employee access to mission-critical applications and data, as well as safeguarding HHS data and systems from unauthorized access and intrusion.

The following examples represent current challenges facing HHS Converged Services, and will continue unabated unless properly addressed:

- Internet and cloud access services continue to utilize an outdated and inefficient traffic model, requiring an overly complicated and expensive process of traversing across multiple systems;
- In accordance with chapter 2170 of the Texas Government Code, HHSC is required to obtain all WAN and Internet services through contracts executed and managed by DIR, who also oversees the entire design of the network. The contracted network service providers typically take a minimum of several months to complete capacity increases or installation of new services. These extended durations severely hinder HHS Converged Services' ability to implement capacity increases in a timely manner that is responsive to system needs;
- An excessive number of networks, service contracts, and other impediments have resulted in unnecessary costs and inefficient processes; and,
- The number of networks in the immediate post-consolidation landscape, combined with a lack of integration of network monitoring and management systems, severely impacts HHS Converged Services' ability to troubleshoot issues across many of the systems currently being utilized to deliver effective and efficient services to HHS programs. Reducing the number of networks and improving integration would help realize the goals of Transformation.

Potential Impact

Network outages or performance degradation issues could have a devastating impact on the ability of programs to perform critical functions. Examples of adverse effects or total system failures resulting from a compromised network infrastructure could include the following:

- Access to cloud platforms that support client service delivery is inhibited, resulting in delayed services, or a total inability to provide services to clients;
- Telework access is compromised, adversely affecting client service delivery and business operations;
- Eligibility and enrollment contact center services become unavailable, precluding enrollment for vulnerable Texans;
- The Texas State Emergency Plan relies on 2-1-1 for critical information dissemination during emergencies, which would go offline in the event of an outage;
- All Voice over Internet Protocol (VoIP) functionality at HHS facilities across the state would be subject to a system-wide outage, which could result in all telephone systems being offline and unavailable;
- Access to state data center services would become unavailable, in addition to HHS internal support systems and client-facing applications; and,
- The provision of services through telemedicine, for rural and vulnerable population subsets would be unavailable in the event of an outage.

Failed network equipment leads to outages and suspension of service delivery at the affected locations. In a practice primarily attributable to budgetary constraints, repairs are often delayed to the point where emergency replacement is the only viable solution. At that juncture, the software is likely no longer supported by the manufacturer, so bug fixes, feature enhancements, and security patches are generally no longer available. Device failure rates will continue to increase and eventually, HHS Converged Services staff will be unable to restore services to office locations due to a lack of available replacement units.

HHS applications traversing the network require the infrastructure and services to comply with numerous laws, regulations, policies, standards, and guidelines. Failure to replace legacy network infrastructure elements jeopardizes the ability of HHS to comply with these requirements, which can contribute to a variety of repercussions, including potential security breaches that could compromise Texans' sensitive data.

Desired Outcome and Future State

An ideal HHS Converged Services environment for the future is based upon a modern architecture that facilitates the efficient coexistence of voice, video, and data systems that are flexible and scalable, with the capacity to expand as business requirements change and grow. This will be accomplished by providing:

- Highly reliable telephony and network environments;
- Continuous adherence to leading security practices;
- Consolidated and standardized hardware that serves the entire system in a cohesive manner;
- Centralized management, monitoring, reporting, and provisioning across all network service infrastructure and systems;
- Direct access to hosted, public, and private cloud platforms from remote sites;
- Remote access support for all HHS telework and mobility initiatives;
- High-quality service for more than 300 critical applications; and,
- Improve application performance and response time over network connections to allow for application acceleration for bandwidth conservation and network performance.

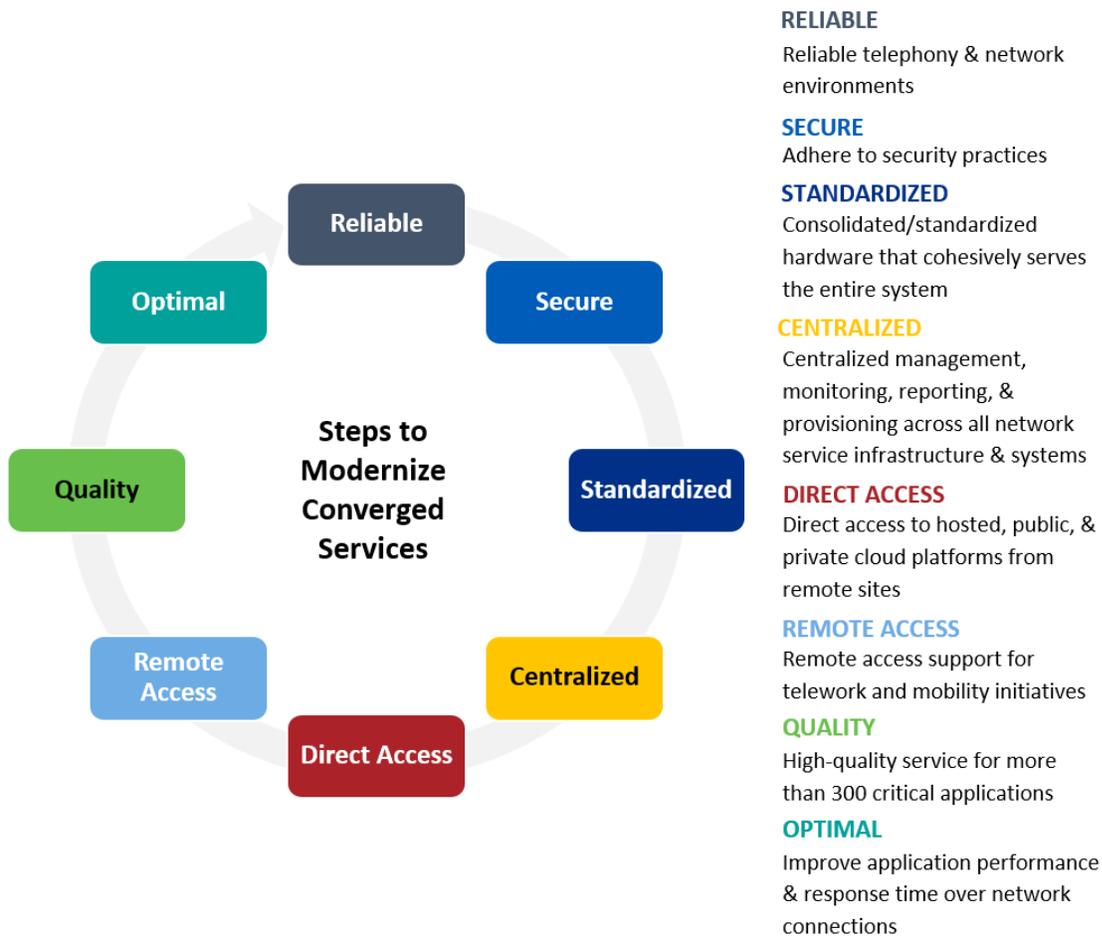
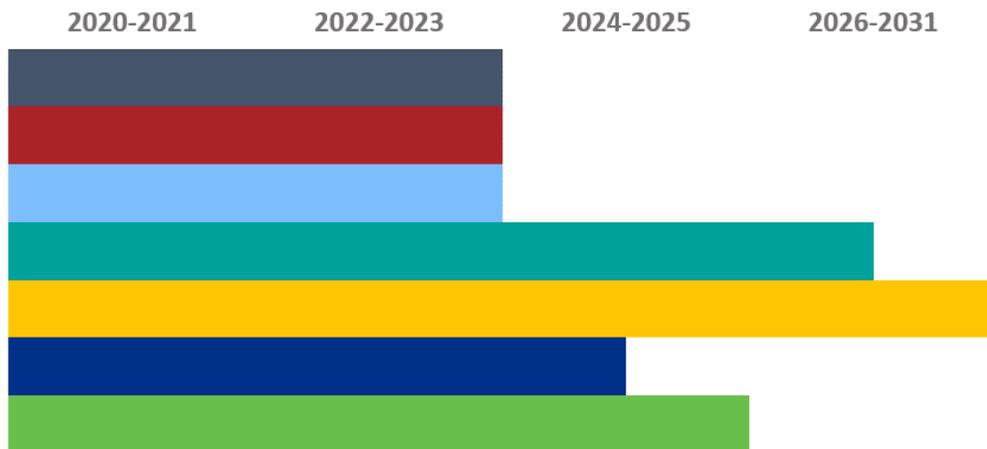


Figure 9 Steps to Modernize Converged Services

Timeline

This section identifies and briefly describes some of the critical components that would drive the effort to modernize the HHS Converged Services network. Accompanying the overview of necessary resources is a projection that details the biennia in which HHS IT leadership currently forecasts the most likely period in which an appropriation request would be presented.



Transition of voice access services to IP-based technologies

- Migration of current legacy voice service to SIP trunks and disconnect of old circuits
- Migration of the legacy voice services at WAN site offices to use existing data network circuits and IP technology
- Retention of vendor services for design and implementation
- Migration to software-defined network (SDN) technologies
- Network infrastructure refresh program
- Redesign of Interactive Voice Response (IVR) systems
- Redesign network elements to support the migration of Avaya Call Center services

Figure 12 Converged Services Timeline

FY 2020 - 2023

The legislature funded an appropriation request in the amount of \$6.3 million for FY 2020-21 to complete the transition of voice access services to IP-based technologies, beginning with a Time-Division Multiplexing (TDM) to Session Initiation Protocol (SIP). TDM technology has been the industry standard for more than 50 years, but with the increasing reliance on high-speed connectivity, the ability to transmit data quickly has resulted in transmission over phone lines becoming nearly obsolete. SIP technology utilizes Ethernet to transfer data at much

faster speeds, providing the flexibility to integrate with cloud platforms, and resulting in significant cost savings due to lesser demand for physical hardware and infrastructure. Such a transition would include the following tasks:

- deployment and integration of SIP trunks on the data network primary access circuits;
- migration of current legacy voice service to SIP trunks and disconnect of old circuits;
- migration of the legacy voice services at WAN site offices to use existing data network circuits and IP technology; and,
- retention of vendor services for design and implementation.

FY 2020 - 2026

The legacy HHS Converged Services network consists of switches, routers, and other devices, each having a single, defined purpose. Migration to software-defined network technologies will help virtualize and synchronize these functions, providing HHS with the flexibility to adapt to frequent changes in system and software requirements without needing to constantly switch out or replace network hardware. This migration will require vendor services for design and implementation.

FY 2020 - 2031

For FY2020-21, the legislature provided \$3,116,000 in base funding for a routine network infrastructure refresh program to be developed and deployed. A proposed renewal of that request has been made for FY 2022-23 in the amount of \$48 million as a subcomponent of a large security EI.

In effort to promote industry best practices, such a program should include the acquisition of core network infrastructure, perimeter security infrastructure, WAN infrastructure, and LAN, all of which require upgrade or replacement with current technology solutions every six to seven years. Vendor services will be needed to assist with the development and implementation of this program.

FY 2022 - 2024

Redesign of Interactive Voice Response (IVR) systems. IVR is an automated telephony system technology that interacts with callers, gathers required information or input from the caller, and routes the call to the appropriate destination. This will involve obtaining the necessary licensing for software and

development tools and will require the retention of vendor services for design and implementation.

FY 2024 - 2025

Network redesign elements will be needed to support the migration of Avaya Call Center services (e.g., call processing, recording, screen capture, reporting, and workforce management) from occurring on site to a hosted cloud platform. This will also require the retention of vendor services for design and implementation.

Benefits to Texans

Even as this plan is published, the world continues to recover from COVID-19 pandemic and respond in a manner that will be sustainable in light of the landscape and new realities of a connected society. With continued support from the Legislature and agency leadership, HHS Converged Services will not only be poised to sufficiently respond to the current and ongoing challenges associated with providing the capacity required to support such a vast network but could even take the more proactive position of designing and implementing a dynamic and robust network that augments and enhances service delivery from program areas across the system. The paradigm of health and human service delivery continues to shift toward a more agile, mobile model, which underscores the importance of a properly designed, highly flexible, and strong network infrastructure.

Client and Agency Computing

Overview and Background

The IT end-user experience is comprised of technologies that manage and secure the systems, devices, applications, and data that an end-user needs to perform their job. These technologies are the essential tools that HHS uses to provide critical services to the citizens of Texas.

Current State

Help Desk

HHS IT Customer Service and Support (CSS) provides incident reporting for IT issues and resolution of HHS staff requests through the HHS IT Customer Service Help Desk. The HHS help desk model uses three methods to collect incidents; phone calls, e-mails, and limited self-service requests, which all require a manual step to resolve.

When an end-user contacts the help desk, the desk creates a ticket for each call or e-mail received. These manual steps can delay the resolution of a help desk ticket. This delay can result in lost time for the individual making the request and potentially impact services to clients as staff are required to wait for the resolution of their ticket to resolve the issue that is preventing them from accomplishing the task at hand.

Onboarding/Offboarding

There is currently no single electronic point of entry during HHS staff onboarding for HHS IT services. Multiple systems, including HR and asset management systems, have limited to no automated interfaces into the onboarding process which results in IT staff manually onboarding resources. The HHS IT help desk submits numerous forms and creates multiple IT work orders. If HHS employee onboarding forms are not provided to the help desk by the hiring manager ahead of time, there is often a delay of two days to one week. During this time, new employees are unable to receive the hardware, software, network, and application access that enables them to perform their job serving HHS clients and the citizens of Texas.

End-User Computing

HHS IT currently services 87-plus variations of PCs and laptops issued to HHS staff. The varieties of models create support challenges, which include deploying essential security patches and operating system updates. To receive these updates, HHS staff must have their computers connected to the HHS network via LAN or VPN to receive application patches and upgrades. When HHS staff do not receive these updates and patches, the computers and applications they use may not work correctly. When HHS staff computers are not updated, delays to HHS client services provided at SSLCs, state hospitals, and Regional Offices can result.

HHS IT also manages 6,000-plus cellular devices for DSHS and HHSC on a Mobile Device Management (MDM) platform that is server-based, this platform presents ongoing issues with aging and requiring ongoing maintenance. If the MDM platform goes down it would leave HHS staff unable to access the tools they need to do their work in the field. These mobile devices allow HHS staff to serve HHS clients from anywhere in Texas.

Collaborative Tools

HHS IT Collaboration & Mobility manages the Office 365 cloud applications for the agency, including Outlook, Skype, Microsoft Teams, amongst others, to enable the agency to communicate and collaborate with each other and clients. The existing environment uses on-premise authentication for Microsoft services. Skype and Microsoft Teams are currently used to meet desktop videoconferencing needs. These collaborative tools give HHS staff the ability to work together to resolve HHS client issues faster and more efficiently.

Desired Outcome and Future State

The goals of the desired outcome and future state for client and agency computing are driven by continuous alignment with industry best practices.

Help Desk Model to Service Desk Model

Implementation of a service desk model is underway to automate less complex IT issues which will allocate CSS staff the capacity to focus on larger customer impacting IT issues and more first call resolutions. The current COVID-19 pandemic and sudden shift to a mobile workforce significantly increased the demand on infrastructure, hardware, and other mobile capabilities. This resulted in unforeseen increased call and email volumes, which are currently beyond CSS resource capabilities. The impact to the help desk is a 40 percent increase in emails (7,000

to 10,000 monthly emails) and a 475 percent increase in the call abandonment rate.

CSS will manage incidents, service requests, and communications from a single point of contact for HHS employees. The service desk will be a division full of resources and individuals with skills and expertise in; incident resolution, work order fulfillment, and problem management. Service desk staff will be responsible for managing customer care and ensuring an overall positive IT end-user experience. This model will enable the implementation of a self-service help desk chatbot to improve the user support experience by providing employees with an automated resource to obtain assistance. The chatbot feature will help improve user productivity and reduce calls to the service desk. Reduced calls to the service desk will provide service desk agents with more time to provide complex troubleshooting and resolution of issues that require increased IT resources. A fully implemented service desk model will enable HHS staff to receive faster resolution of IT issues and requests allowing them to focus on providing services to HHS clients.

Onboarding/Offboarding

An automated onboarding solution will streamline employee onboarding, offboarding, relocation, leaves of absence, and other processes that directly affect IT services. Automated employee onboarding will reduce the delays currently experienced and optimizes staff productivity by allowing them to perform their job duties and training on their first day at HHS. This onboarding solution also ensures that HHS staff have appropriate access to the systems, networks, devices, and software needed based on their role within the enterprise. It will also remove resources immediately upon an individual's departure from HHS employment, which ensures that HHS client data remains safe.

End-User Computing

A reduced variation in computer models will enable HHS staff to spend less time adapting to the use of different computer models and ease and streamline HHS IT's management of PCs and laptops. Lease expirations and manufacturing lifecycles will provide the basis of the reduction in the variety of models. The provision of Microsoft Windows as a service will allow users the ability to update their computers with flexibility and ease. This service reduces security risks and downtime from malfunctioning applications. Fewer types of computer models will streamline the implementation of a PC cloud management solution and classification and protection of HHS client data in the cloud. One result of the COVID-19 response is the implementation of contactless processes that allow HHS staff to receive their

equipment at a depot and with the ability to begin working as soon as a connection is made to a wireless network. Another is HHS IT collaboration with vendors to ensure HHS staff mobility and access to the accessories required to do their work.

Collaborative Tools

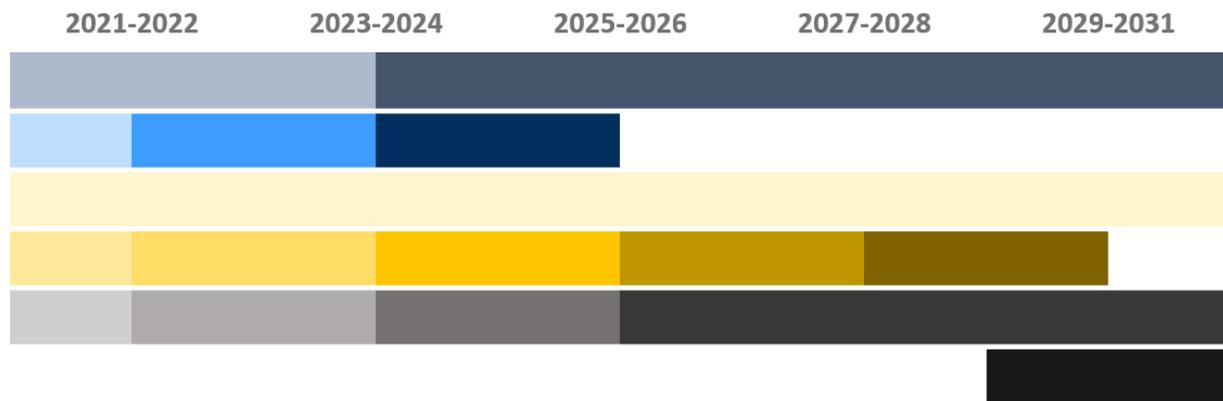
Full agency adoption of Microsoft Modern Desktop tools will enhance HHS staff collaboration and productivity. Because these collaborative tools do not require specialized hardware or operating systems, they can work with different types of systems without compatibility issues. For example, an HHS employee working from home coordinating COVID-19 pandemic contact tracing volunteers lost internet connectivity from their internet service provider. These tools enabled that HHS employee to securely use their smartphone and an Apple laptop without compromising security to coordinate volunteers using Microsoft web-based applications as if they were using Microsoft desktop applications on a PC.

Microsoft Modern Desktop tools will simplify IT support and enable automation of processes and prevent functionality and security issues for the agency by making it easier to keep these tools up-to-date. As Mobile Device Management moves to a cloud-based solution, there will be additional capabilities for “Bring Your Own Device” support, which utilizes a self-service approach to streamline integration of mobile devices used by HHS staff and will allow them even more flexibility in how and where they are able to serve Texans.

As the agency adoption of these tools moves forward through strategic training and adoption programs, HHS staff will have the ability to work and collaborate with HHS clients from any location. This ability will enable HHS staff to be even more person-centered in their work with HHS clients.

Timeline

The completion of this timeline is dependent on funding. HHS IT uses a continuous quality improvement (CQI) process, which allows for the review of new technologies in order to make sure those new technologies align with modern business requirements. Every item in the timeline below uses the CQI process for technology reviews.



HELP DESK MODEL TO SERVICE DESK MODEL

- Implement service desk model and identification of a self-service chatbot solution
- Review new technologies for alignment with modern business requirements

ONBOARDING/OFFBOARDING

- Identify HHS enterprise onboarding/offboarding solution
- Implement onboarding/offboarding solution with role-based processes
- Complete the implementation of role-based onboarding

END-USER COMPUTING

- Continue deployment of laptops and other mobile hardware
- Complete the implementation of Microsoft services in the Office 365 cloud environment
- Begin the utilization of cloud services
- Deploy security patches and application updates from the cloud
- Complete cloud services implementation
- Review HHS technologies to align with business requirements
- Begin building virtualized environment to support "Bring Your Own Device" (BYOD) program
- Continue and finish building the cellular virtual BYOD environment program
- Initiate full virtualization of end-user cellular environment
- Complete full virtualization of the end-user cellular environment completed
- Review HHS technologies to align with business requirements

COLLABORATIVE TOOLS

- Continue adopting MS Modern Desktop tools
- Migrate all desktop video conferencing to MS Teams
- Continue implementing additional security configurations & automated provisioning from FY 2020
- Initiate Mobile Device Mgmt migration to the cloud
- Complete full adoption of existing and new MS Modern Desktop tools
- Complete security configurations & automated provisioning
- Complete Mobile Device Management migration to cloud
- Review business requirements
- Prepare Office 365 integration with legacy cloud apps
- Complete Office 365 integration with legacy cloud apps
- Introduce new tools and review technologies to ensure alignment with business requirements
- Propose the implementation of new technologies to remain aligned with current business requirements as part of the end-user computing continuous improvement plan

Figure 10 Client and Customer Services Timeline

Help Desk Model to Service Desk Model

FY 2020 - 2021

Begin implementation of the service desk model and identification of a self-service chatbot solution.

FY 2022 – 2023

Implementation of the service desk model and self-service chatbot solution complete by the end of FY2023.

Resources Required

FY 2022 - 2023

Contract Services

- Third-party vendor for a chatbot solution
 - Financials undefined

FY 2024 - 2029

- Review new technologies for alignment with modern business requirements as part of a continuous improvement plan.

Onboarding/Offboarding

FY 2020 - 2021

- Begin identification of an HHS enterprise onboarding/offboarding solution.

FY 2022 - 2023

- Begin and complete implementation of an HHS enterprise onboarding/offboarding solution and begin implementation of roles-based onboarding. HHS job profiles will be standardized for all end users in a phased approach for the implementation of roles-based onboarding.

FY 2024 - 2025

- Continue and complete the implementation of roles-based onboarding.

Resources FY 2022 -2025

Projected resources required for future business requirements.

- Training budget \$15,000
- Four FTEs
 - Onboarding project implementation
 - ◇ One Project Manager II for HHS job profile standardization
 - ◇ One Project Manager III for roles-based resource assessment
 - ◇ Two System Analyst V for roles-based resource assessment

End-User Computing

FY 2020 - 2021

- Complete the implementation of Microsoft services in the Office 365 cloud environment, dependent on Microsoft OneDrive implementation, and begin the utilization of cloud services to classify and protect end-user data.
- Begin and complete deployment of security patches and application updates from the cloud. This will allow HHS staff to connect and download those patches and updates from anywhere with an internet connection.

FY 2020 - 2031

- Continue deployment of laptops and other mobile hardware to the HHS workforce, dependent on current lease expirations and the refresh schedule.

FY 2022 - 2023

- Continue and complete the implementation of cloud services to classify and protect end-user data.
- Review HHS technologies to align with business requirements.
- Begin building the virtualized environment to support the "Bring Your Own Device" program.

FY 2024 - 2025

- Continue and finish building the cellular virtual environment for the "Bring Your Own Device" program.

FY 2026 - 2027

- Full virtualization of the end-user cellular environment begins.

FY 2028 - 2029

- Full virtualization of the end-user cellular environment completed. Review HHS technologies to align with business requirements.

Resources FY 2022 - 2031

Projected resources required for future business requirements.

- Training budget \$100,000, averaging \$10k per year
- Nine FTEs
 - ▶ System Configuration Management
 - ◇ Three System Analyst V
 - ◇ Two System Analyst VI
 - ▶ Seat/SAM Management
 - ◇ Three System V
 - ◇ One Budget Analyst

Contract Services

- Services provided by Third Party resources to support End User Computing
 - ▶ Financials undefined

Collaborative Tools

FY 2020 - 2021

- Continue with full HHS adoption of Microsoft Modern Desktop tools.
- Begin and complete the migration of all desktop video conferencing (i.e., Skype) to users in Microsoft Teams.
- Continue the ongoing implementation of additional security configurations and automated provisioning and administration from FY 2020.
- Begin the migration of Mobile Device Management to a cloud-based platform.

FY 2022 - 2023

- Continue and complete the full HHS adoption existing and new Microsoft Modern Desktop tools.
- Continue and complete additional security configurations and automated provisioning and administration.
- Complete the Mobile Device Management migration to a cloud-based platform.
- Review business requirements to ensure the HHS technology strategy remains aligned with changing business needs.
- Begin focusing on the integration of Office 365 with legacy applications that moved to the cloud.

FY 2024 - 2025

- Complete the integration of Office 365 with legacy applications that moved to the cloud.

FY 2026 - 2031

- Introduce new collaboration tools to HHS and review technologies to ensure alignment with business requirements.

Resources FY 2022 - 2031

- Training budget \$10,000
- Five FTEs
 - ▶ Project Management for the implementation of cloud-based projects
 - ◇ One Project Manager III
 - ▶ Integration of Office 365 with legacy applications and support of net new applications
 - ◇ Two System Analyst V
 - ▶ E-mail and Cloud Security Implementation, Operations, and Reporting
 - ◇ One System Analyst V
 - ◇ One System Analyst VI

FY 2030 - 2031

Propose the implementation of new technologies to remain aligned with current business requirements as part of the end-user computing continuous improvement plan.

Benefits to Texans

These improvements to the end-user experience will give HHS front-line staff an available, reliable, and fast system that will allow them to provide services and responses quickly to HHS clients. HHS staff will be able to begin work immediately and experience less downtime when there are issues with equipment and applications. The enhanced collaboration will allow staff to resolve HHS client policy issues quickly. These kinds of enhancements will allow for quick issue resolution between HHS staff, contractors, providers, and HHS clients.

Workforce

Current State

Technological, social, and labor market changes have made workforce demands more complex and dynamic, leading to a significant shift in skill and talent needs. This shift has made it increasingly difficult to recruit and retain appropriate staff to fill critical IT positions. HHS IT is focusing on effective management and stewardship, including technology investments, as a primary goal. These priorities are based on the recognition that insufficient data sharing, legacy systems, and inefficient technical processes are holding back HHS's ability to serve the public better and ensure a new future for health care in Texas.

Currently, HHS IT has a total of 1,173 FTEs out of 1,414 available positions. The types of positions in IT include:

- Administrative Support (10);
- Budget Analysts (4);
- Clerical (8);
- Contract Managers (6);
- Contract Specialists (7);
- Data Architect (1);
- Database Administrators (29);
- Directors (57);
- Financial Analysts (17);
- Managers (60);
- Network Specialists (199);
- Program Specialists (37);
- Programmers (69);
- Project Managers (37);
- Systems Analysts (703);
- System Support Personnel (139); and,
- Telecommunication Personnel (25).

All positions and employees play an integral role in providing outstanding customer service and innovative technology solutions securely, efficiently, and effectively.

The current turnover rate in IT is 14.12 percent, with a vacancy rate of 16.17 percent. The average annual salary for active IT employees is currently \$70,067, compared to the average annual salary of HHS IT personnel in Austin of \$68,074.

For Programmers, which is one of the most difficult to fill IT positions, the average annual salary in HHS is \$86,828, compared to the average annual salary in Austin of \$88,657.

IT Workforce Support launched their recruitment function in February 2019 to support the self-service model currently in use at HHS. Due to these efforts, the average time from posting to hire for IT positions the Workforce Support team assisted with was reduced from 64 days to 45 days.

One of our priorities is to enhance the skills of our current workforce. One way we have achieved this objective is by purchasing LinkedIn Learning licenses for all IT staff. LinkedIn Learning gives employees access to world-class content. They offer high-quality, professionally produced content that is relevant to staff and have built a highly engaging learning experience that exceeds the high expectations of modern learners. Their robust learning platform allows both employee-driven and management-driven education to build a culture of continuous learning in our organization.

Desired Outcome and Future State

The desired outcome for the HHS IT workforce is to have the ability to:

- Identify critical roles with talent-shortage risks based on external and internal talent-supply data;
- Provide benchmarking and labor market insights on talent availability, sourcing costs, and market competition when implementing the organization's strategic goals;
- Incorporate timelines for talent acquisition into action steps to ensure project plans for strategic goals are set with realistic expectations of the time required to obtain the necessary talent;
- Understand hiring needs for the future and resource properly against anticipated demand; and,
- Prepare for potential challenges when hiring for critical roles, begin sourcing and pipeline building, and work with leadership to identify and ensure the agency obtains the talent needed to meet its strategic goals.

To achieve this result, we plan to implement the strategic workforce plan below:

IT STRATEGIC WORKFORCE

Planning Process



A strategic workforce plan is a long-term blueprint to ensure workforce optimization—a holistic strategy encompassing recruiting, developing, managing, remaining, and redeploying talent to maximize the effectiveness of both the current and future workforce in light of strategic business priorities.

The IT Strategic Workforce Planning Process includes the following:

- Understand Change Drivers
 - ▶ Identify IT implications of business strategy.
 - ◇ Translate high-level corporate goals into IT objectives, and map current IT capabilities to these objectives.
 - ▶ Analyze external trends.
- Analyze external factors and macro-level workforce trends that may impact the business and IT talent pipeline.
- Identify Impact on IT Talent
 - ▶ Identify Competency and Skill Requirements
 - ◇ Derive talent implications from the IT objectives to prepare for changes in the IT workforce plan.
 - ▶ Identify IT Tole Shifts
 - ◇ Highlight critical current and future skills and roles and map the competencies that drive high performance to these roles.

- ▶ Define Outsourcing Potential
- ▶ Define which skills and roles can be outsourced to calibrate the allocation of internal and external resources.
- Diagnose Talent Gaps
 - ▶ Assess Your Current Team
 - ◇ Evaluate core competencies and strategy-critical skills to understand the strengths and weaknesses of the IT organization.
 - ◇ Forecast Openings
 - ◇ Identify attrition risk and redirect new openings to ensure the timely and effective development and acquisition of talent.
- Attract the Best Talent
 - ▶ Create an Attractive EVP
 - ◇ Explicitly communicate core drivers of the IT employment value proposition (EVP) to competitively hire and retain talent.
 - ▶ Proactively Source Candidates
 - ◇ Evaluate diverse sourcing channels and design the steps IT will take to proactively generate qualified leads.
- Build the Best Talent
 - ▶ Identify HIPOS
 - ◇ Identify and communicate with high-potential employees to motivate and develop them for future leadership positions.
 - ▶ Design a Succession Strategy
 - ◇ Identify talented leaders and provide development experiences to help them take up future leadership positions.
 - ▶ Create Development and Training Plans
 - ◇ Invest in strengthening the competencies and skills to build the next generation of world-class IT professionals.

The optimal workforce environment will include highly skilled and quality HHS IT staff, training and development opportunities, appropriate placement of skilled personnel, reduced time to hire, and high retention rates. To reach this ideal state, the following efforts will be accomplished:

- Identification of talent needs well in advance to avoid last-minute “desperation” hires;
- Assessment of team core competencies and strategy-critical skills to understand the strengths and weaknesses of the IT department;
- Forecast openings to identify attrition risks and predict new openings, ensuring timely and effective development and acquisition of talent;
- Proactively source candidates. Evaluate diverse sourcing channels and design the steps IT will take to proactively find talent;
- Identification of high-performing employees to motivate and develop them for future leadership positions;
- Establishment of a succession strategy by identifying talented leaders and providing development experiences to help them assume future leadership positions;
- Creation of development and training plans to build the competencies and skills of the next generation of world-class professionals; and,
- Evaluation of processes and procedures, measuring and communicating effectiveness and progress toward talent goals on an ongoing basis.

Achievement of these efforts will ensure HHS has extensive resources and adept individuals with the progressive skills and expertise required to fulfill the many essential functions vital to HHS operations.

Resources Needed

Investment in development and training plans will be needed to strengthen the competencies and skills of HHS professionals, to include:

- Tool specific training (SAS, Tableau, etc.);
- Skill specific training (data literacy, performance measurement, etc.);
- Agile coaching and education for HHS IT and non-IT staff; and,
- Incident response and problem management capabilities.

Conclusion

Texas HHS is committed to achieving operational excellence by enacting efficient and effective business practices and processes. The IT division has continued to evolve to meet the needs of diverse programs, employees, and clients. HHS aims to leverage and expand on our current IT modernization and improvement efforts to make the best use of every taxpayer dollar the agency is appropriated to maximize outcomes for Texans.

For the FY 2022-23 biennium, the agency proposes the following EIs for consideration to support our 10-year IT and Data Services Modernization Plan as outlined above.

Agency	Funding Request Name
HHSC	Maintain Compliance with Federal Data Governance Requirements and Maintain Data Driven Decision Making
HHSC	CAPPS Compliance and Stabilization
DSHS	Community Health, Product Safety, Regulatory Automation System Functionality
DSHS	COVID-19 Vaccine Infrastructure ImmTrac Enhancements
DSHS	Data Center Consolidation
HHSC	Electronic Visit Verification Expansion
DSHS	EMS and Trauma Registries
HHSC	Foster Care Litigation
DSHS	Funding to Support the Operation of the Texas Center for Infectious Disease
HHSC	Comply with Federal Requirements for Community Integration for Individuals with Disabilities

Agency	Funding Request Name
HHSC	IDD System Redesign and Waiver
HHSC	IT Security Threat Reduction and System Stabilization
HHSC	OIG Beneficiary Fraud Data Analytics Platform
HHSC	OIG Case Management System
HHSC	Phase 1: MMIS Modernization Procurement and Timeline
DSHS	Public Health Frontier, Health Rural Public Health Clinics and Mobile Public Health Clinics
DSHS	Public Health Frontier, System Infrastructure, Public Health Clinic Electronic Health Records
HHSC	Stabilize E-Discovery

List of Acronyms

Acronym	Full Name
AD	Active Directory
AES	Access & Eligibility Services
AI	Artificial Intelligence
ASOIG	Automated System of the Office of Inspector General
BEP	Business Enablement Platform
BLSSE	Blood Lead Surveillance System Efficiency
BOP	Biennial Operation Plan
BYOD	Bring Your Own Device
CADS	Center for Analytics and Decision Support
CARE	Client Assignment and Registration System
CDA	Chief Data Architect
CDAO	Chief Data & Analytics Officer
CHIP	Children's Health Insurance Program
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMBHS	Clinical Management for Behavioral Health Services
CMS	Center for Medicare and Medicaid Services
COTS	Commercial Off-the-Shelf
COVID-19	Coronavirus Disease 2019
CPRO	Chief Policy & Regulatory Officer
CQI	Continuous Quality Improvement
CRM	Customer Relationship Management
CSOC	Cybersecurity Operations Center
CSS	Customer Service and Support
CTO	Chief Technology Officer

DADS	Department of Aging and Disability Services
DARS	Department of Assistive and Rehabilitative Services
DCIO	Deputy Chief Information Officer
DCS	Data Center Services
Dev/Ops	Development/Operations
DFPS	Department of Family and Protective Services
DGPM	Data Governance and Performance Management
DIR	Department of Information Resources
DSHS	Department of State Health Services
eCommerce	Electronic Commerce
EDG	Enterprise Data Governance program
EDW/BI	Enterprise Data Warehouse/Business Intelligence
EI	Exceptional Item
EMS	Emergency Medical Services
EOSL	End-of-Service Life
ERP	Enterprise Resource Planning
ESC	Executive Steering Committee
EVP	Employment Value Proposition
FERPA	Family Educational Rights and Privacy Act
FTE	Fulltime Employee
FTI	Federal Tax Information
FY	Fiscal Year
GRC	Governance, Risk, and Compliance
HB	House Bill
HHS	Texas Health and Human Services
HHSC	Health and Human Services Commission
HIPAA	Health Insurance Portability and Accountability Act
HSCS	Health & Specialty Care System
IaaS	Infrastructure as a Service

IAM	Identity and Access Management
I-APD	Implementation Advance Planning Document
IDD	Intellectual or Developmental Disability
IDD CARE	Intellectually Disabled Client Assignment and Registration System
IDD-BHS	Intellectual or Developmental Disability and Behavioral Health Services
IoT	Internet of Things
IRM	Information Resources Manager
IR	Information Resource
IRIS	Integrated Resident Information System
IT	Information Technology
ITIL	IT Infrastructure Library
ITSM	Information Technology Services Management
IVR	Interactive Voice Response
KPIs	Key Performance Indicators
LAN	Local Area Network
LIMS	Laboratory Information Management System
LOI	Local Office Infrastructure
MCO	Managed Care Organization
MCS	Medicaid & CHIP Services
MDM	Mobile Device Management
MFADS	Medicaid Fraud and Abuse Detection System
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information Systems
MPLS	Multi-Protocol Label Switching
NAA	Network Access Administrative
NEDSS	National Electronic Disease Surveillance System
NIST	National Institute of Standards and Technology
Office 365	Microsoft Office 365

OIG	Office of Inspector General
OP	Office of Performance
PAI	Performance and Analytics Integration
PHI	Protected Health Information
PII	Personally Identifiable Information
PM	Performance Management
PMAS	Performance Management and Analytics System
PMD	Performance Management Dashboard
PMO	Project Management Office
ROI	Return on Investment
RPA	Chat Bots and Robotic Process Automation
RSD	Regulatory Services Division
SaaS	Software as a Service
SB	Senate Bill
SIP	Session Initiation Protocol
SNAP	Supplemental Nutrition Assistance Program
SPI	Sensitive Personal Information
SSLCs	State Supported Living Centers
SSS	System Support Services
SWI	Statewide Intake
TAC	Texas Administrative Code
TANF	Temporary Assistance for Needy Families
TDM	Time-Division Multiplexing
TIERS	Texas Integrated Eligibility Redesign System
TMHP MMIS	Texas Medicaid and Healthcare Partnership Medicaid Managed Information System
TxEVER	Texas Electronic Vital Events Register
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

WAN	Wide Area Network
WIC	Women, Infants, and Children
WLAN	Wireless Local Area Network