NC DEPARTMENT OF HEALTH AND HUMAN SERVICES
Information Technology Division

Cloud Computing Strategy

Last Update	*October 24, 2019*
Author	*Corey Mercy*
Contributors	***Sam Gibbs, Charles Carter, Angela Taylor, Steve Tedder, Iris Cooper, Jessie Tenenbaum, Reese Edgington, Jennifer Braley, Bill Morton, Pyreddy Reddy***
Revision	***Initial***
Next Revision	***Annually (at minimum)***

Table of Contents

Executive Summary

The purpose of this document is to define and communicate the North Carolina Department of Health and Human Services (NCDHHS) unified direction and strategy on cloud computing services adoption. This document seeks to identify high-level adoption approaches and methodologies that are agreed upon by all impacted stakeholders.

Cloud computing as we know it today began in 2006 when Amazon Web Services (AWS) introduced their Elastic Compute Cloud. Since that time, numerous other technology companies have introduced a plethora of cloud service offerings. Private and public sector entities have been rapidly migrating to the cloud to recognize the multitude of benefits cloud computing offers.

Our vision is to conduct the majority of our business via cloud computing by 2025. We believe that cloud computing services are uniquely positioned to support our strategic technology requirements now and in the future. With cloud computing, we plan to achieve the following business goals.

- Allow business owners dealing with legislative mandates that appear with little or no time to react to test their business plans more quickly for relatively little initial cost.
- Achieve faster reaction to the changes that occur due to federal, state, department, or division needs that are often outside our control.
- Enhance our ability to react to changing compute needs
- Establish a more reliable and highly available technology footprint with reduced capital investments.
- Accelerate the decommission of existing NCDHHS data centers.

With that said, cloud services adoption will impose new challenges for our department which we plan to address as follows:

- We will build decision frameworks to select appropriate cloud services and providers based on the level of control we require and a set of agreed baseline criteria.
- We will develop an exit strategy for the cloud providers that will host our mission-critical workloads and we will pursue multicloud strategies to distribute the risk across multiple vendors.
- We will integrate the NCDHHS network infrastructure with our primary cloud providers to ensure performance and confidentiality.
- We will protect our data using encryption whenever possible and utilize encryption key management solution that is FIPS 140-2 level 2/level 3 compliant.
- We will implement the federal, state, NCDHHS privacy and security compliance requirements as directed by the regulatory requirements.

Cloud services will require NCDHHS to transform and acquire new skills and processes that we don't currently possess. To facilitate the adoption of cloud services, we will build a Cloud Center of Innovation, and Cloud Advisory Council which will execute our cloud strategy and will establish the policies and principles that govern our cloud services usage. Furthermore, we will develop decision frameworks for governing the following aspects:

- The migration priority for existing applications based on risk, benefit, efforts and feasibility.
- The migration strategy for existing applications. We will prefer the "rehost" approach to accelerate adoption, but we won't discourage approaches such as "rearchitect" or "rebuild" when the return on investment (ROI) is positive in the medium term (three to five years).
- The optimal application placement between public cloud providers and applicable NC Department of Information Technology (DIT) data centers.

This collaborative engagement of stakeholders across the Department, along with our partnership with DIT, in support of a cloud-first strategy will help ensure success in our endeavors and better position NCDHHS for the future.

Business Objectives

Vision

NC Department of Health and Human Services will conduct more than 60% of our business via cloud technologies by 2025. To support this vision, NCDHHS will require a highly scalable, resilient, innovative and elastic infrastructure and technology platform.

Our current IT footprint and resources cannot meet the agility and scalability needs that we expect to require in the near future. Adapting our current IT to support existing and future digital business needs is anti-economical and would require significant capital investments in nonstrategic assets such as data centers, and excess infrastructure. Conversely, we believe that public cloud services are well positioned to support the current and future strategic technology requirements of NCDHHS and our respective divisions. By nature, cloud computing services are scalable, programmable, resilient, and available on-demand, with no need to undertake long-term capital investments.

Key objectives are to:

- Reduce overall operational costs through cloud infrastructure efficiencies that enable supply and demand for environments and employ elastic cost base and transparency;
- Lower costs by eliminating the current ongoing need for hardware refresh and constant maintenance;
- Improve workforce productivity through access to cloud services and mitigating the delay to acquire timely environment access;
- Improve operational and business agility by enabling NCDHHS to react to federal, state, and business changes more quickly through acquisition of flexible cloud compute resources necessary to meet the requirements as well as providing additional optional solutions to address these changes; and
- Improve the security posture of NCDHHS by implementing workloads in the cloud using Federal Risk and Authorization Management Program (FEDRAMP), Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA) compliant cloud services.

Two-year targets include:

- Decommission data centers in the Harvey and Bath Buildings; in Division of State Operated Healthcare Facilities (DSOHF) such as the Alcohol and Drug Abuse Treatment Centers (ADATC): Julian F. Keith, R.J. Blackley and Walter B Jones; Developmental Centers: Caswell, J. Iverson Riddle and Murdoch; Neuro-Medical Treatment Centers: Black Mountain, O'Berry and Longleaf and the Residential Programs for Children: Wright School and Whitaker Psychiatric Residential Treatment Facility.
- Implement Cloud Backup Solution to replace disk and tape backups
- Migrate North Carolina Families Accessing Services through Technology (NC FAST), Preadmission Screening and Resident Review (PASRR), and some DSOHF services to the cloud
- Build and deploy additional Medicaid Modules to the cloud
- Cloud first approach for all new projects

To support this business vision, our Department will adopt cloud computing services according to the strategy outlined in this document.

Goals and Benefits

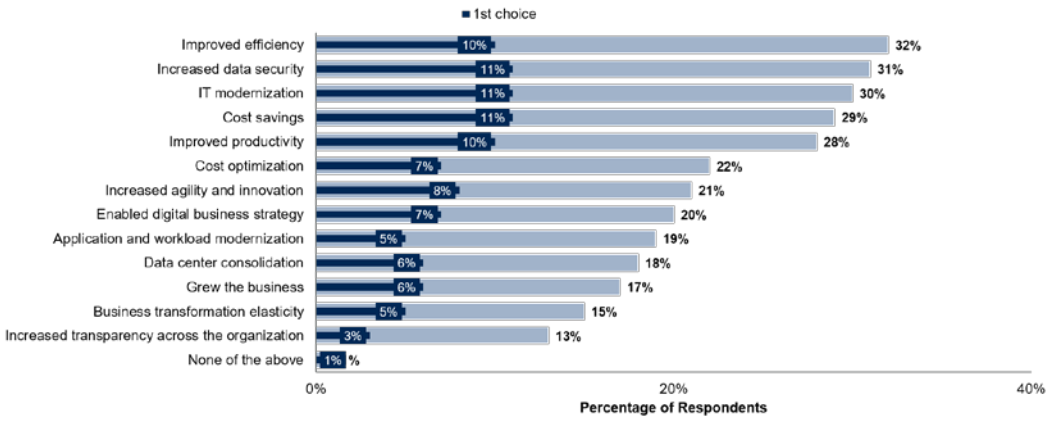
NCDHHS has adopted and committed to a cloud-first strategy. Cloud will become our primary and preferred deployment model for all IT workloads. If there are compelling reasons not to use cloud computing, we will address these needs using DIT's hybrid cloud and data centers. However, as part of our cloud-first approach, we plan to accelerate the decommissioning of existing NCDHHS data centers, as they are considered nonstrategic assets for our department.

We expect that the adoption of cloud services will bring the following business and technical benefits to our agency, both inside and outside of IT:

- Allows business owners dealing with legislative mandates that appear with little or no time to react to test their business plans more quickly for relatively little initial cost.
- Faster reaction to the changes that occur due to federal, state, department, or division needs that are often outside our control.
- More transparency around the costs of IT and how these costs are aligned to specific division services.
- Reduce IT costs by eliminating the need for buying unused capacity and deploying applications which take advantage of cost savings technologies like containers and serverless architecture.
- Ability to serve rapid increases in demand, even when these exceed our provisioned capacity.
- Ability to accelerate delivery of new projects and enhancements.
- Increased productivity by shifting our IT personnel away from managing data centers toward higher-value tasks.
- Ability to achieve cost savings on infrastructure.
- Ability to more quickly recognize the benefit of new technologies as they are released by cloud providers.
- Improved availability of our applications to our customers due to more reliable and secure architectures in cloud providers.
- Enhance our ability to react to changing workloads without having to manage or over provision our capacity requirements.
- Fostering innovation by providing the infrastructure and access to emerging cloud native services to team members when needed for testing their ideas.

Other State and Federal Agencies, such as Arizona, Maryland, CMS, ONC, HHS, and numerous others have already embarked on their cloud adoption journey and are reporting success. A 2018 Gartner survey with almost 1,000 respondents across industries and geographies indicated that most organizations report successful outcomes from the adoption of cloud services. A breakdown of the reported outcomes is outlined in Figure 1.

Figure 1. Gartner Survey 2018: Reported Successful Outcomes of Cloud



Success Metrics

To determine the effectiveness of this cloud strategy at achieving our Departmental goals, we will measure our cloud implementation process against the metrics in Table 1. We will also conduct, at a minimum, a biannual assessment of our progress against these metrics in order to make adjustments to the implementation plan as needed.

Table 1. Success Metrics

Goal	Metric	Success Value
Accelerate Delivery of Enhancements	Average Months from Idea to Working Prototype	4 months
Increase New Cloud Initiatives or Projects	Number of New Initiatives or Projects	3 per year
Increase Infrastructure Cost Savings	USD	22%
Establish Cost Transparency	Number of Workloads with Effective Cost Tracking	10 per year

Risk Assessment

We have identified the following risks related to the adoption of cloud services. The list has been collectively built with input from infrastructure and operations, application development, security, networking, identity, legal and procurement. These risks and mitigations strategies are listed in Table 2.

Table 2. Risk Assessment and Mitigation

Perceived Risk	Mitigation Strategies		
Internal resistance to cloud adoption	Seek executive sponsorship	Trigger compelling event (such as deadline for data center exit)	Manage cloud community program to influence behavior and transform internal culture
Don't possess the required skills	Build training program to develop the required skill set	Seek advice and recommendations of an MSP/professional services organization	Seek research and advisory services
We store data that contains confidential PII, PHI, IRS, SSA, CMS and VA information[1]	Implement cloud security best practices (such as microsegmentation security posture management and security as code)	Develop cloud data protection and access control by developing data and security governance polices.	Build decision framework to select cloud provider with the understanding of the provider supports for federal and state regulatory requirements (such as HIPAA, PCI, and FERPA).
We may overspend in the cloud	Develop financial management processes for public clouds	Assign and enforce budget limits on a per-workload basis	Use cloud provider quotas to limit the number of resources we can provision
We may experience challenges moving from a capex to an opex budget and funding model	Develop budget management and funding process which support opex model	Seek guidance from other states who have made this transition	Develop strategy for opex funding in new initiatives and enhancements

[1] HHS Office of the Secretary, Office for Civil Rights, & Ocr. (2017, June 16). Cloud Computing. Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

We may experience WAN outages due to DIT or Third-Party Service Provider maintenance or unplanned outages	Establish direct connections with cloud service providers	Ensure redundant WAN connections to all NCDHHS locations utilizing different telco providers.	Ensure WAN network has no single points of failure and differing service providers are utilized for primary and secondary paths.

A more complete and detailed risk assessment and mitigation effort will be performed as part of the implementation plan.

Organizational Impact

To be successful with our cloud first strategy, NCDHHS must transform. Our current skill sets, roles and organizational structures are not optimal for the cloud computing model. Cloud services require a higher level of autonomy and self-service for end users than what we provide today in our highly centralized IT model. Furthermore, cloud services require the governance of a number of configuration options.

While transforming our department is necessary, this transformation also constitutes a challenge in and of itself. This is due to the natural resistance to change and the lack of skills with the new technologies that we are planning to adopt. As a result of this, we are planning to:

- **Establish a cloud center of innovation (CCOI):** A team of dedicated Cloud Architects, the CCoI will become a core resource of cloud expertise and knowledge within the Department. The team's role will include governance, compliance, consulting and project engagement. Cloud Architects will have areas of specialization, in addition to knowledge of various cloud providers services, implementation strategies, and frameworks for designing successful cloud solutions. The CCoI will also be responsible for partnering with various Divisions and business functions to ensure the necessary operational process and tools are in place for managing and monitoring clouds operations (i.e., cost management, template repository, utilization, and performance).
- **Establish a cloud advisory council (CAC):** The cloud advisory council will be chaired by the Deputy CTO and Deputy CIO. It will be led by the CAC Coordinator. Members will include the operational areas across the Information Technology Division, Privacy and Security, Finance, Legal, Procurement, Human Resources, key Division Representatives, and DIT. The council will be responsible for ensuring the CCOI is progressing smoothly with cloud adoption and remove any roadblocks or difficulties. They will also ensure cross-function collaboration to provide the CCOI with necessary resources and partnerships to enable cloud adoption. The CAC will authorize all policies related to cloud computing, respond to governance reports, and determine the future direction of the CCOI based on the cloud strategy.
- **Prepare to scale our DevOps practice:** Shifting our DevOps practice to more effectively support cloud computing will involve continued adoption and maturation of agile development processes. In addition, our practices must focus on simplifying application code deployment, automating software release processes, and testing. This will include focus on provisioning and managing infrastructure, as well as monitoring application and infrastructure performance
- **New Departmental Initiatives and Projects:** As new initiatives and projects procure solutions to meet departmental needs, we will need to establish new, and revise existing processes (like NCDHHS Information Technology Governance Board (ITGB) and Enterprise Architecture) to ensure appropriate integration and implementation of these new cloud solutions. Additional focus in leveraging these new and innovative solutions offered by cloud solutions will also need to be employed.
- **Transform IT into a broker of cloud services:** The role of a service broker is to enable developers, consumers and Divisions to quickly access technology services while safeguarding the Department through the application of centralized policies and procedures. Efforts will need to be undertaken to transform from the traditional central IT functions to partnering in the vetting, implementation, and adoption of cloud solutions.

Training and Certification

We plan to acquire the required technical skills through vendor-specific cloud certification programs and training. These training and certification programs require commitment and time investment of the staff involved. Courses range from 1 to multiple days and certification exams require extensive preparation.

Because the acquisition of the required skills will take time, we also plan to address our short-term needs (especially during the migration phase) through outside consulting resources and short-term staffing as needed.

Table 3 shows the certification programs that we intend to leverage to acquire cloud skills.

Table 3. Cloud Provider Certifications

Cloud Provider	Certification Program
Amazon Web Services	Cloud Practitioner
Amazon Web Services	Developer
Amazon Web Services	Solution Architect
Amazon Web Services	SysOps Administrator
Amazon Web Services	DevOps Engineer
Amazon Web Services	Security
Amazon Web Services	Advanced Networking

(AWS Training and Certification https://aws.amazon.com/training/?nav=tc&loc=1)

Cloud Provider	Certification Program
Microsoft Azure	Azure Administrator Associate
Microsoft Azure	Azure Security Engineer Associate
Microsoft Azure	Azure Data Engineer Associate
Microsoft Azure	Azure Developer Associate
Microsoft Azure	Azure DevOps Engineer Expert
Microsoft Azure	Azure Solutions Architect Expert

(Microsoft Azure Learning https://www.microsoft.com/en-us/learning/default.aspx)

Cloud Provider	Certification Program
Google Cloud Platform	Associate Cloud Engineer
Google Cloud Platform	Professional Data Engineer
Google Cloud Platform	Professional Cloud Developer
Google Cloud Platform	Professional Cloud Security Engineer
Google Cloud Platform	Professional Cloud Network Engineer
Google Cloud Platform	Professional Collaboration Engineer

(Google Cloud Platform Training: https://cloud.google.com/training/)

As we mature our multicloud strategy we will also expand the certification programs we engage in to ensure necessary knowledge and skill sets are in place.

Business Process

We also plan to adapt our existing processes to accommodate for the characteristics of cloud computing. At a minimum, we plan to adapt the following:

- **Procurement.** In a cloud computing environment technology provisioning occurs in a self-service, on-demand fashion. Existing procurement processes and polices will need to be reviewed and revised to accommodate this shift in procurement capability.
- **Operations.** Current Infrastructure & Operations functions are structured to provision and maintain services within NCDHHS and/or DIT owned data centers. In adapting to a cloud computing model, I&O will need to establish processes, frameworks, and tools for managing cloud computing resources. The initial approach will prioritize leveraging cloud provider native tools.
- **Infrastructure Resource provisioning.** Historically when provisioning hardware resources they have always been sized for peak load and future growth. In this practice of sizing resources typically there is a significant amount of over provisioning and overspending. With our move to cloud computing our practice will need to shift to sizing for exactly what capacity is needed, with the ability to scale the resources when needed, and enable/disable capacity on-demand.
- **Budgeting and forecasting.** Current budget and forecasting occurs on a biennial cycle with significant capex investments for technology initiatives with limited visibility in to operational service costs at a granular level. In cloud computing, cost models will largely shift to opex with potentials for fluctuation from one month to the next. Specific consideration and efforts will need to be placed on cost management, forecasting demand, and understanding ongoing consumption needs to enable the most effective approaches to managing costs (shutting down resources when not needed, purchasing reserve and spot instances, etc.)

Decision Governance

Cloud services will require a number of decisions throughout the adoption process and, later, on an ongoing basis once we are fully onboard with cloud services usage. This cloud strategy document does not intend to state and agree on all the decisions we'll have to make. However, this document intends to identify a few key decisions and define the core principles that will regulate these decisions once we move forward with the implementation.

The core decisions and the leading questions that are discussed in this cloud strategy document are listed in Table 4.

Table 4. Key Cloud Adoption Decisions

Area	Decision Question
Cloud-first	Will we adopt a cloud-first policy?
Application assessment	How do we assess our existing applications against cloud migration?
Security strategy	How do we implement the security and privacy requirements (vulnerability management, access controls, etc) in the cloud?
Application migration strategy	Which migration strategy will we adopt?
Cloud tiers	How do we decide between Software as a Service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS)?
Cloud providers	How do we select a cloud provider?

Multicloud	Will we pursue a multicloud strategy from the start?
Hybrid IT	How do we integrate our on-premises data center?
Workload placement	How do we select the best environment for net new workloads?

Cloud-First

The NC Department of Health and Human Services is adopting a cloud-first strategy.

Application Assessment

Work is currently underway with the application rationalization initiative started by the Application Project Management Office (APMO). As this work progresses, we will ensure questions are included with regards to current SaaS solutions as well as details concerning data exchange, type of data stored, and complexity of code base. Any new concepts or initiatives presented to ITGB will be required to answer these questions.

Security Strategy

Our strategy includes continuous monitoring to detect malicious activity using vulnerability scanning tools; performing risk analysis against NIST 800-53 rev 4 security controls; implementing security controls to identify, prevent and detect threats using code as well as security indents and event management (SIEM) tools to automate response and recovery procedures for threats using industry proven procedures.

Application Migration Strategy

The application portfolio across the Department consists of a multitude of commercial off the shelf, custom built, and in-house developed applications of varying complexity and age. As we evaluate each application for migration to the cloud our considerations will included whether to take the approach of rehost, revise, rearchitect, rebuild, or replace the tool.

Cloud Tiers

Our strategy includes leveraging all tiers of cloud provisioning. Software as a Service will be considered first for every application being evaluated for migration to the cloud. Where there are no appropriate SaaS solutions, we will then look at Platform as a Service solutions to meet the operational needs of the workload. Finally, Infrastructure as a Service will be evaluated and deployed when there are no suitable SaaS or PaaS options.

Cloud Providers

Currently the Department has workloads with Amazon Web Services (AWS), Appriss, ServiceNow, Smartsheet, and Microsoft. AWS hosts NC-Treatment Outcomes and Program Performance System (NC-TOPPS) for the Division of Mental Health/Developmental Disabilities/Substance Abuse Services (DMH/DD/SAS); Encounter Processing System (EPS), PHP Contract Data Utility (PCDU), and Managed File Transfer (MFT) for the Division of Health Benefits-NC Medicaid. Appriss hosts the Controlled Substances Reporting System (CSRS) for DMH/DD/SAS. ServiceNow hosts IT Service Management (ITSM) for the Department through DIT. Smartsheet provides NCDHHS Human Resources access to their tools through their SaaS and AWS offering. Microsoft hosts Office 365 for the Department.

Multicloud

NCDHHS' long-range plan is to leverage multiple clouds in the placement and delivery of our workloads. However, leveraging multiple cloud providers introduces numerous operational complexities[2]. To manage this risk, and in consultation with Gartner experts, the initial stages of our cloud computing strategy will focus on minimizing complexities and maximizing access to the right technology.

[2] Meinardi, M. (2019). Designing a Cloud Strategy Document. Stamford, CT: Gartner.

In all cases we will have clear exit strategies defined for each of our cloud workloads.

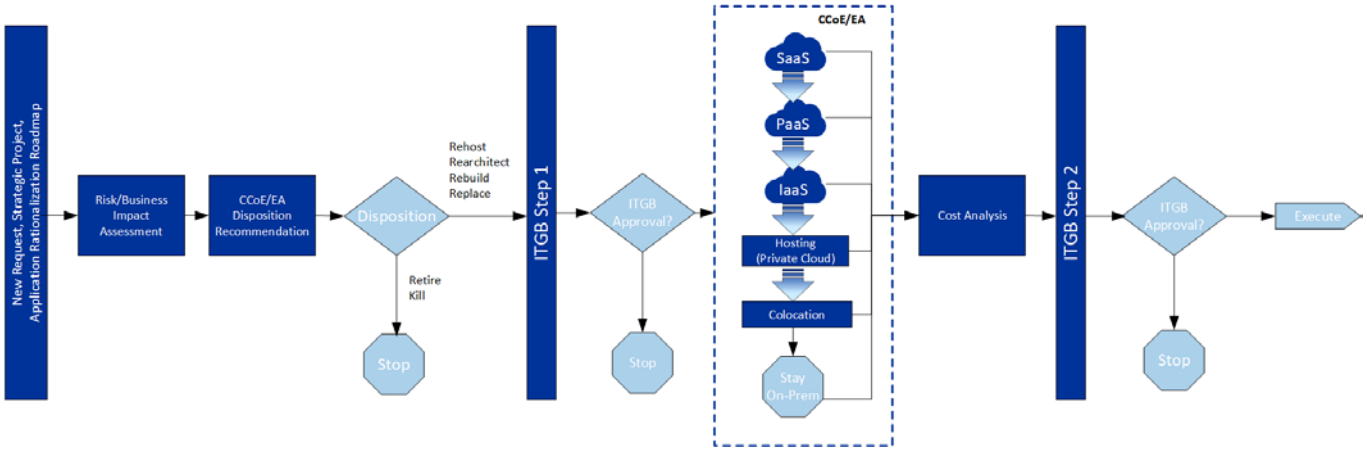
Hybrid IT

While NCDHHS data centers have been designated as nonstrategic assets in our cloud-first strategy, we acknowledge there may be legacy computing needs which require extended transition planning and considerations. Placement, or retention of workloads in on-premise environments will be evaluated on a case by case basis with the intention of migrating to one of the DIT data centers.

Workload Placement

Workload placement will be determined based on the priority and criticality of the workload. Figure 2 provides a framework by which we will evaluate each workload to determine the most appropriate technology solution. After moving through the initial gates of evaluation and risk assessment, our approach will start with evaluation of SaaS offering and work down through the cloud tiers. Hosting options would include DIT's VMWare data center extension service. Where workloads absolutely require deployment to an on-premise solution, we will leverage the DIT Eastern and Western data centers with the intent of eliminating all NCDHHS owned data centers.

Figure 2. Workload Placement Decision Framework



Follow-Up

The scope of this cloud strategy document has been kept intentionally tight and focused on the key principles, constraints and requirements that the North Carolina Department of Health and Human Services must consider as we decide to adopt cloud services. In partnership with the North Carolina Department of Information Technology, we are planning to follow with more detailed and execution-focused documentation as we mature in our cloud adoption knowledge and experience.

Signatures

This cloud computing strategy document has been drafted collaboratively throughout the organization. We have involved and consulted key stakeholders who are distributed across all affected departments, inside and outside of IT.

By providing their signature in Table 5 below, stakeholders confirm hereby that this cloud strategy document responds to the needs of the business and that they agree on the decision to move forward with the implementation of cloud services according to this cloud strategy.

Table 5. Approval Signatures

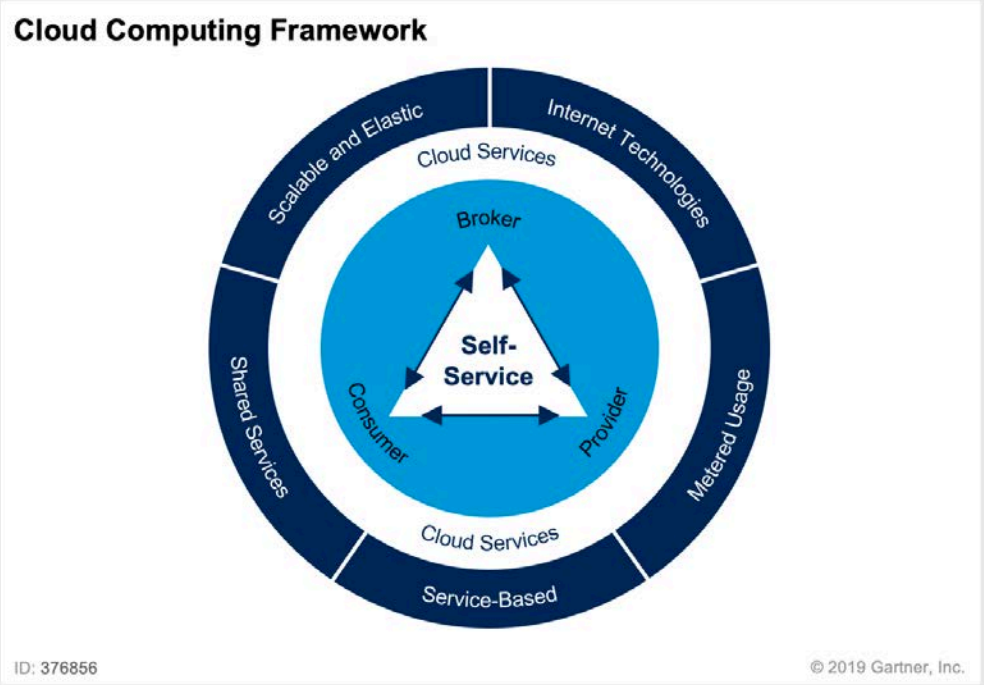
Printed Name	Role	DHHS Division	Signature
Corey Mercy	Deputy Chief Technology Officer (CAC Co-Chair)	Information Technology Division	DocuSigned by: Corey Mercy FCADB3FBE5204E9...
Reese Edgington	Deputy Chief Information Officer (CAC Co-Chair)	Information Technology Division	DocuSigned by: Reese Edgington C4847B7193344D6...
Mark Benton	Director	Division of Public Health	DocuSigned by: Mark T. Benton 85A1EF320AD0418...
Iris Cooper	Assistant Secretary	Office of Procurement, Contracts & Grants	DocuSigned by: Iris Cooper F0A1B988148B439...
Patrick Doyle	Director, Business Information & Analytics	Division of Health Benefits - NC Medicaid	DocuSigned by: Patrick Doyle 37EB28ABAD3F42B...
Rob Morrell	Director, Business Information Office	Human Services	DocuSigned by: Rob Morrell 75E9CEFC9E6E484...
Bill Morton	Infrastructure Director	Information Technology Division	DocuSigned by: Bill Morton A39ACEF222FD48B...
Beth Roberts	Acting Budget Officer	Information Technology Division	DocuSigned by: Beth Roberts F2E5DF1A88E94AD...
Pyreddy Reddy	Chief Information Security Officer	Information Technology Division	DocuSigned by: Pyreddy Reddy [illegible]
Jessie Tenenbaum	Chief Data Officer	Office of the Secretary	[illegible] 4806A47558D04BC...
Helen Wolstenholme	Director	Division of State Operated Healthcare Facilities	DocuSigned by: Helen Wolstenholme 0C56943103FC4B6...

APPENDIX

Cloud Defined

"A style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies."

Figure 3. Cloud Computing Framework



To be considered a cloud service, a solution should adhere to some combination of the attributes defined below and provided in Figure 3:

- **Service-Based:** Consumer concerns are abstracted from provider concerns through service interfaces that are well-defined. The interfaces hide the implementation details and enable a completely automated response by the provider of the service to the consumer of the service. In addition, the service could be considered "ready to use" or "off the shelf" because the service is designed to serve the specific needs of a set of consumers, and the technologies are tailored to that need rather than the service being tailored to how the technology works. The articulation of the service feature is based on service levels and IT outcomes (availability, response time, performance versus price, and clear and predefined operational processes), rather than technology and its capabilities. In other words, what the service needs to do is more important than how the technologies are used to implement the solution.
- **Scalable and Elastic:** The service can scale capacity up or down as the consumer demands at the speed of full automation (which may be seconds for some services and hours for others). Elasticity is a trait of shared pools of resources. Scalability is a feature of the underlying infrastructure and software platforms. Elasticity is associated with not only scale but also an economic model that enables scaling in both directions in an automated fashion. This means that services scale on-demand to add or remove resources as needed.

- **Shared:** Services share a pool of resources to build economies of scale. IT resources are used with maximum efficiency. The underlying infrastructure, software or platforms are shared among the consumers of the service (usually unknown to the consumers). This enables unused resources to serve multiple needs for multiple consumers, all working at the same time.
- **Metered by Use:** Services are tracked with usage metrics to enable multiple payment models. The service provider has a usage accounting model for measuring the use of the services, which could then be used to create different pricing plans and models. These may include pay-as-you go plans, subscriptions, fixed plans and even free plans. The implied payment plans will be based on usage, not on the cost of the equipment. These plans are based on the amount of the service used by the consumers, which may be in terms of hours, data transfers or other use-based attributes delivered.
- **Uses Internet Technologies:** The service is delivered using internet identifiers, formats and protocols, such as URLs, HTTP, IP and representational state transfer web-oriented architecture.

Furthermore, cloud computing declines in three different tiers, specifically:

- **Infrastructure as a Service (IaaS).** IaaS is a standardized, highly automated offering in which computing resources owned by a service provider, complemented by storage and networking capabilities, are offered to customers on demand. Resources are scalable and elastic in near real time and metered by use. Self-service interfaces, including an API and a graphical user interface (GUI), are exposed directly to customers. Resources may be single-tenant or multitenant, and are hosted by the service provider or on-premises in a customer's data center. Examples of IaaS offerings include Amazon Web Services, Microsoft Azure and Google Cloud Platform.
- **Software as a Service (SaaS).** Software that is owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics. Examples of SaaS offerings include Microsoft Office 365, Salesforce and Workday.
- **Platform as a Service (PaaS).** A PaaS is usually depicted in all-cloud diagrams between the SaaS layer above it and the IaaS layer below, is a broad collection of application infrastructure (middleware) services (including application platform, integration, business process management and database services). However, the hype surrounding the PaaS concept is focused mainly on application PaaS (aPaaS) as the representative of the whole category. Examples of PaaS offerings include Aws Lambda, Google App Engine and Oracle Cloud Platform.

Cloud computing services can be provided using the following deployment models:

- **Public cloud computing.** A style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using internet technologies — i.e., public cloud computing uses cloud computing technologies to support customers that are external to the provider's organization. Using public cloud services generates the types of economies of scale and sharing of resources that can reduce costs and increase choices of technologies. From a government organization's perspective, using public cloud services implies that any organization (in any industry sector and jurisdiction) can use the same services (e.g., infrastructure, platform or software), without guarantees about where data would be located and stored.
- **Private cloud computing.** Private cloud computing is a form of cloud computing that is used by only one organization, or that ensures that an organization is completely isolated from others.
- **Hybrid cloud computing.** Hybrid cloud computing refers to policy-based and coordinated service provisioning, use and management across a mixture of public and private cloud services.
- **Multicloud computing.** Multicloud computing refers to the use of cloud services from multiple public cloud providers for the same purpose. It is a special form of hybrid cloud computing.