COUNTY OF LOS ANGELES
DEPARTMENT OF HEALTH SERVICES

LAC+USC
Medical Center

INFORMATION TECHNOLOGY STRATEGIC PLAN

FY 2022-2024

TABLE OF CONTENTS

Contents

EXECUTIVE SUMMARY

The Information Technology Strategic Plan (ITSP) has been developed to support the Strategic Business Plan by assembling and applying the information resources that are necessary to achieve the strategic objectives. ITSP is aligned with DHS Strategic Plan and ensures that those linkages are highlighted throughout. This ITSP is organized into four categories.

I. Information Technology Mission and Vision Statement
II. Information Technology Objectives
III. Information Systems Organizational Structure
IV. Scope of Information Technology Services

I. INFORMATION TECHNOLOGY MISSION AND VISION STATEMENT

Mission

To effectively align business objectives and Information Technology (IT) at LAC+USC Medical Center in support of the Department of Health Services' Mission. To provide the most advanced technology in support of the delivery of patient care services.

Vision

To provide flexible, efficient, and secure modern information technology that enables the Medical Center and its partners to respond to the requirements of their missions.

II. IT OBJECTIVES

The ITSP is aligned with DHS Strategic plan by defining the below objectives to deliver effective and measurable operational Results.

- Operational Efficiency
- Information Security
- Enterprise Applications
- IT Workforce Development

1. Operational Efficiency

Enterprise Helpdesk:

Serves as the first level support for technical assistance and support for incoming queries and issues related to computer systems, software, and hardware regardless of which DHS location users are calling from. The Enterprise Helpdesk implements process improvement strategies that support IT best practices framework. They ensure consistent/uniformed ticketing and monitor help desk functions across the DHS Enterprise. They streamline tiered IT dispatched support from a consolidated centrally managed service environment.

Enterprise Network Operations Center
The Enterprise Network Operations center is manned 24/7 from a tiered support mechanism. The support personnel monitor and manage alerts of the DHS network and infrastructure and assigns routine tasks to IT analyst across the enterprise. They also notify and alert technical teams when system outages occur in an emergent manner.
The Enterprise Network Operations Center team provides 24/7 monitoring of all DHS to ensure networks are up and running smoothly, and with no interruptions. If there is a problem, they can instantly detect the issue and reach out to the correct team to have the issue resolved. This proactive approach allows IT Operations to resolve issues prior to user impact. The Enterprise NOC team can detect and reach system owners 24/7, if a mission critical system fails system owners will be notified afterhours and issues can be resolved prior to the next business day and reduce impact to patient care.

Enterprise Change Management
The Enterprise Change Management is responsible for managing all changes to the Production Operations and infrastructure environment from inception to completion. The DHS Enterprise Change Management team ensures all changes are recorded and authorized at the appropriate level within IT and the Business without being overly bureaucratic.

Types of Changes:

- Standard: A routine task that is performed without risk at a specified interval with a script that is well defined; or an activity that has an approved procedure (Standard Operating Procedure “SOP”) and previously authorized by the CAB.
- Normal: A change that will require significant effort and may have a substantial impact on services. Or A change that requires significant effort and coordination, and will likely pose negative impact to systems and services (i.e., service interruption)
- Emergency: A change that requires immediate attention to avoid a service impacting incident/event. Emergency changes use excessive resources due to their unexpected nature should be avoided if possible. Verbal approval may be appropriate to reduce operational impact.

Enterprise Problem Management
DHS Problem Management Team is process responsible for managing the lifecycle of all problems (Major Incident) that happen or could happen in an IT service. The primary objectives is to prevent problems and resulting incidents from happening and to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.

Problem Management includes the activities required to diagnose the root cause of incidents identified through the Incident Management process, and to determine the resolution to those problems. Team is responsible for ensuring that the resolution is implemented through the appropriate Change Management procedures. Team will also maintain information about problems and the appropriate workarounds and resolutions, so that the organization is able to reduce the number and impact of incidents over time.

Problem Management works together with Incident Management and Change Management to ensure that IT service availability and quality are increased. When incidents are resolved, information about the resolution is recorded. Over time, this information is used to speed up the resolution time and identify permanent solutions, reducing the number and resolution time of incidents. This results in less downtime and less disruption to business-critical systems.

Endpoint Management

Endpoint Management team has the oversight to implement organizational governance, industry standards, and best practices relevant toward maintaining and delivering consistent and effective operational IT practices and security requirements to all desktop endpoints deployed at LAC+USC. Including the oversight of security patching to ensure that all IT security policies are up to date, deployed, revised, and maintained. This team is responsible for discovering endpoint desktop security gaps, they ensure that all devices are hardened, compliant, and monitored to provide around the clock security and operational efficiency.

2. Information Security

Information security safeguards are in place in the form of Administrative, Technical, and Physical to protect Protected Health Information (PHI) and other confidential information.

Administrative

Access, Integrity and Confidentiality

Confidential access is provided to clinicians and administrative personnel through several channels including paper files, online systems, and system reports. LAC+USC protects confidential data and information in either hardcopy or electronic form. Information is used for patient care, research, or administrative processes. The confidentiality and integrity of information is supported through the adherence to network policies and procedures.

Role Based Security

Access to information and information systems is governed by “role based” security principles. Access is based on job level, function, and level of security authorization. Security management identifies users access information, the information accessed, the sensitivity of the information, and the security of transmission.

Application System Security

Application systems at LAC+USCHCN include application security that requires the entry of a unique username/code and a password. Application security is used in conjunction with network operating systems and client operating system mechanisms.

Health Insurance Portability Accountability Act (HIPAA)

The Health Insurance Portability Accountability Act (HIPAA) regulates the confidentiality and portability of patient data. Mandates on the security and privacy of patient and health care data are having a significant impact on information distribution and management. The act consists of three parts: a) regulations, b) transactions and code sets, and c) privacy and security.

Technical

Web/Internet Technologies

Web based technologies continue to drive the development of technology. This includes a range of technologies and services such as intranets/extranets, XML, ASP (Application Service Providers) services and Web Services.

Security Technologies

Network & Workstation security requirements are proving more necessary due to the constant development of viruses, worms, internal and external threats, and unauthorized access to system and network resources.

Portable Computing devices

USB drives, laptops, PDA Based Personal Digital Assistants (PDAs) or handheld computers are making inroads into the traditional standalone personal computer market as the need for mobility and portability influence the type of computing device used by health practitioners.

Wireless Computing

A companion technology with hand-held computing, wireless technologies (802.11) are evolving and are becoming more prevalent in health care settings that demand wireless mobility.

Physical

Access to Restricted IT Areas

Physical security measures are in place to prevent physical tampering, damage, theft, or unauthorized physical access to LAC+USC data center. Access to data centers, computer rooms, telephone closets, network router and hub rooms, and similar areas containing I/T resources are restricted to authorized workforce members with identifiable badge requirements.

Surveillance

Additional physical security control such as CCTV cameras are in place on all data center perimeters.

3. Enterprise Business Applications and Development

The Enterprise Business Applications and Development Support team is dedicated in providing support to our medical staff, business, and financial units by leveraging available Information Technology solutions and training. This is realized by connecting healthcare services and charge capture to claims submissions to optimize reimbursement and financial reporting. The following services are:

- Management of the Affinity RCO financial applications system
- The onboarding and sustainable training of ancillary and medical staff
- Management of patient enrollment data
- Data Analytics and Ad Hoc reporting
- Development and management of Budget Allocation Tools
- Support of day-to-day operations through web development and in house solutions

4. IT Workforce Development

Focus on overall growth and development of IT staff into specialists, analysts, project managers, subject matter experts, and leaders with DHS and beyond. Various training opportunities are made available for improvement of skillsets and knowledgebase of workforce. IT wellness

III. INFORMATION SYSTEMS ORGANIZATIONAL STRUCTURE

The Medical Center's Information System Department consists of the following divisions and sections:

- **Enterprise Infrastructure & Operations Division**
- **Departmental IT Security Office**
- **Clinical Systems**
- **Enterprise Applications & Development**
- **Medical Library Services**

IV. SCOPE OF INFORMATION TECHNOLOGY SERVICES

The Enterprise Infrastructure & Operations Division core activities are:

- Server Administration
- Software and Hardware Maintenance
- Application Evaluation, Testing, and Implementation Hardware and Software
- Deployment and Upgrade Data Network Infrastructure Wireless Network
- Infrastructure Telephone System
- IP Telephony System
- Technical/PC Support
- Service Desk Operation
- Information Technology Training
- Cellular Phones and Pager Operation
- Telephone Operator Operation
- IT Hardware and Software Procurement

Departmental IT Security Office

- Administrative
- Technical
- Physical

Clinical Systems

- Clinical Application Implementation and development
- Clinical Application Education and Training

The Enterprise Applications & Development Division core activities consist of:

- Implement Commercial Off The Shelf (COTS) Systems
- Development and implementation of in-house Clinical Applications
- Database management services
- Database migration
- Systems Integration
- Systems administration and maintenance
- Querying service operations
- Financial Application Support
- Applications and Development
  - Programming and development
  - In-house Application Development
  - Clinical Interfaces
  - Systems Integration
  - Enterprise SharePoint Development
  - Database Management and Reporting
  - Web Portal (Intranet and Internet) development and maintenance

V. CONCLUSION

This document outlines IT goals across four interrelated IT categories:

- Information Technology Mission and Vision Statement
- Information Technology Objectives
- Information Systems Organizational Structure
- Scope of Information Technology Services

The objectives outlined in the ITSP will support, the Medical Center's Information Systems department to succeed in providing world-class IT service in support of DHS mission, goals, objectives, and strategies. Information Systems department will also have remained aligned with any changes in DHS direction. Many steps are necessary to arrive at that future. This document represents the first step of a continual process that requires collaboration and communication across the LAC+USC Medical Center and DHS. It also serves as the baseline for guiding the Information Systems in support of DHS and in its mission to be a center of excellence across the County of Los Angeles.