

Solution Architecture

Executive Summary

To provide a Single Sign-On (SSO). Background: Single Sign-On (SSO) has been identified by ITS leadership as a key initiative to enable a unified, seamless computing environment. Password resets constitute the highest call volume to the Resolution Center; approximately 10,000 calls per month for Corporate alone.

- Request: Develop a Single Sign-On Solution Architecture for the workforce.
- Current State SSO:
 - Web SSO: None
 - Enterprise SSO (ESSO):
 - Imprivata OneSign:
 - Re-authentication capabilities to meet the Ohio State Board of Pharmacy requirements (as required by Cerner).
 - System Office and Resolution Center
 - Caradigm Vergence – multiple locations
- Future State SSO:
 - Web SSO:
 - Utilize a single solution for Web SSO. NetIQ has been selected and purchased, as the enterprise standard.
 - Enterprise SSO (ESSO):
 - Utilize Enterprise SSO (ESSO) for use cases that cannot be addressed by Web SSO, e.g., shared workstations, re-authentication, etc.
- Next Steps:
 - Assess the current environment to prioritize applications and use cases for both Web SSO and ESSO.
 - Select ESSO solution(s).
 - Implement Web SSO and ESSO solutions.
 - Approve NetIQ as the Web SSO enterprise standard.
 - Review Roadmap.

Impacts:

- Business Owners
- ITS Function Leaders
- Information Owners
- Human Resources
- Application Owners
- Technology Services
- Technology Owner
- Technology Services
- Customer Support
- IT Service Mgmt.

Definitions

Single Sign-On (SSO) is the users' ability to login using their ID / PW once and then automatically login to other pre-defined target applications.

Web Single Sign-On (Web SSO):

- Web Access Management (WAM) is a mainstream technology solution providing single sign-on (SSO) for Web applications.
- Identity Federation is a mainstream technology solution that leverages standard protocols to provide single sign-on for Web apps and allows identities to be shared between disparate organizations and applications.

Enterprise Single Sign-On (ESSO) enables the user to login once to a workstation and then automatically login to a mix of pre-defined applications including web, thick, and thin clients.

- Usually, ESSO tools also meet shared workstations and re-authentication needs.

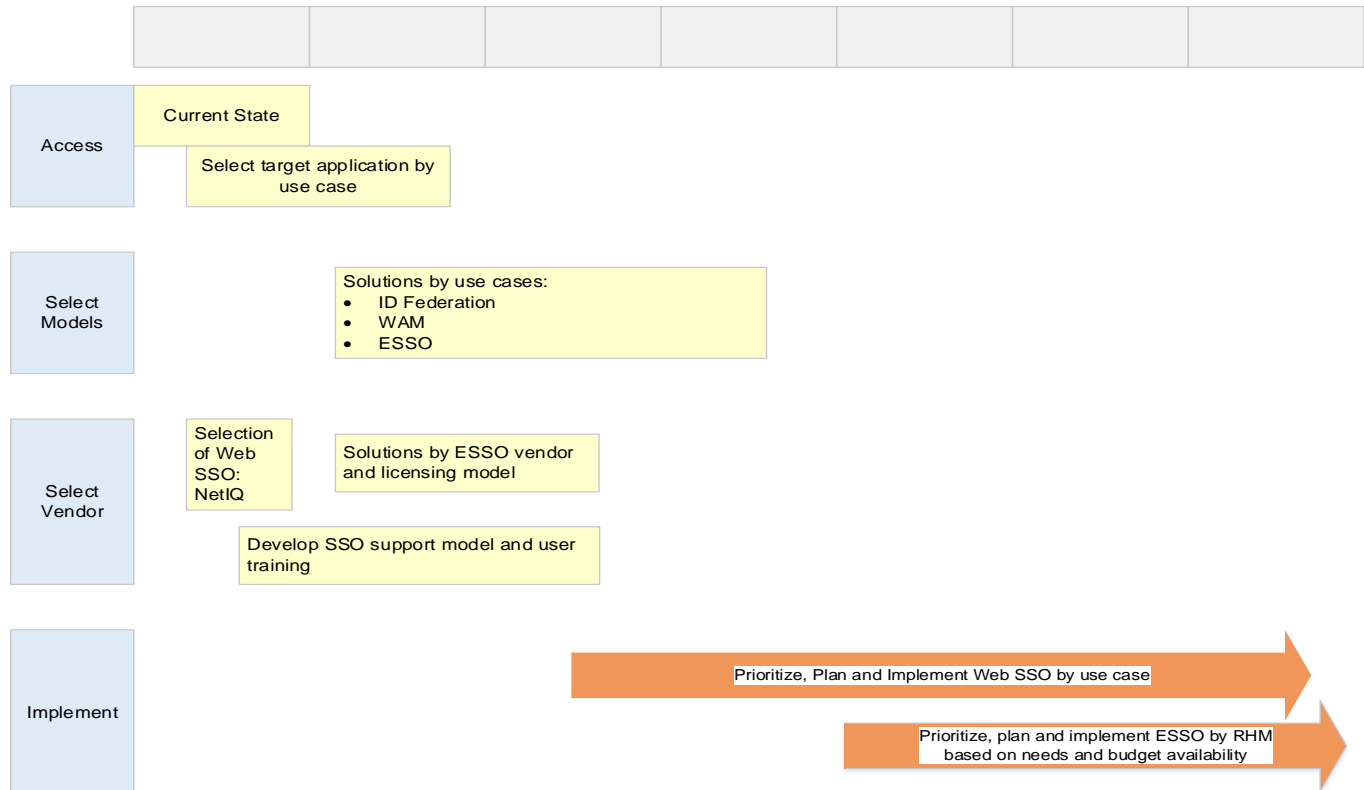
Reduced Sign-On (RSO) is the ability to manually login to multiple applications using the same ID / PW.

Background

A buildup of target applications requires users to login multiple times with multiple passwords.

- Workstation and Application access is cumbersome and time-consuming for users, especially for clinicians.
- Password resets constitute the highest call volume to the Resolution Center; approximately 10,000 calls per month for Corporate alone.
- Multiple passwords lead to unsecure password practices, such as writing down passwords.
- Corporate currently has three (3) solutions to provide SSO:
 - NetIQ,
 - Imprivata,
 - and Caradigm.
- Visual Integration using MPages is also used to meet SSO needs in Cerner.
- Mount Carmel implemented the Imprivata OneSign solution to provide SSO and re-authentication capabilities to meet the Ohio State Board of Pharmacy requirements (as required by Cerner).
- Implemented Caradigm Vergence in the clinical areas of multiple locations.
- Corporate has chosen NetIQ for Web SSO (WAM and ID Federation).
- Adoption of software as a service (SaaS) applications has become the most common driver for new SSO solutions.
- The market for SSO products, which use an agent to push user IDs and passwords into the user interfaces of target applications, has slowly declined, but there is more demand for SSO tools that integrate with Web-architected applications and support identity federation.
- ESSO tools are still needed in some use cases such as shared workstation support that allows rapid user switching or the need for re-authentication.
- Through 2023, federated SSO will be the predominant SSO technology needed by 80% of enterprises.

High Level Roadmap



Summary

- Single Sign-On (SSO) is a major colleague satisfier, especially for clinicians who need to login to multiple applications several times a day.
- Possible SSO solutions include:
 - Web SSO: WAM or ID Federation.
 - ESSO.
- NetIQ Access Manager has been selected as the Web SSO (WAM and ID Federation) enterprise standard solution.
 - NetIQ is the industry leader in the Identity and Access Management market.
 - NetIQ is the Corporate Division Identity Management Solution. Has no Identity Management Solution.
 - Corporate Division already owned some licensing for NetIQ Access Manager.

ESSO is still needed for shared workstations or for re-authentication.

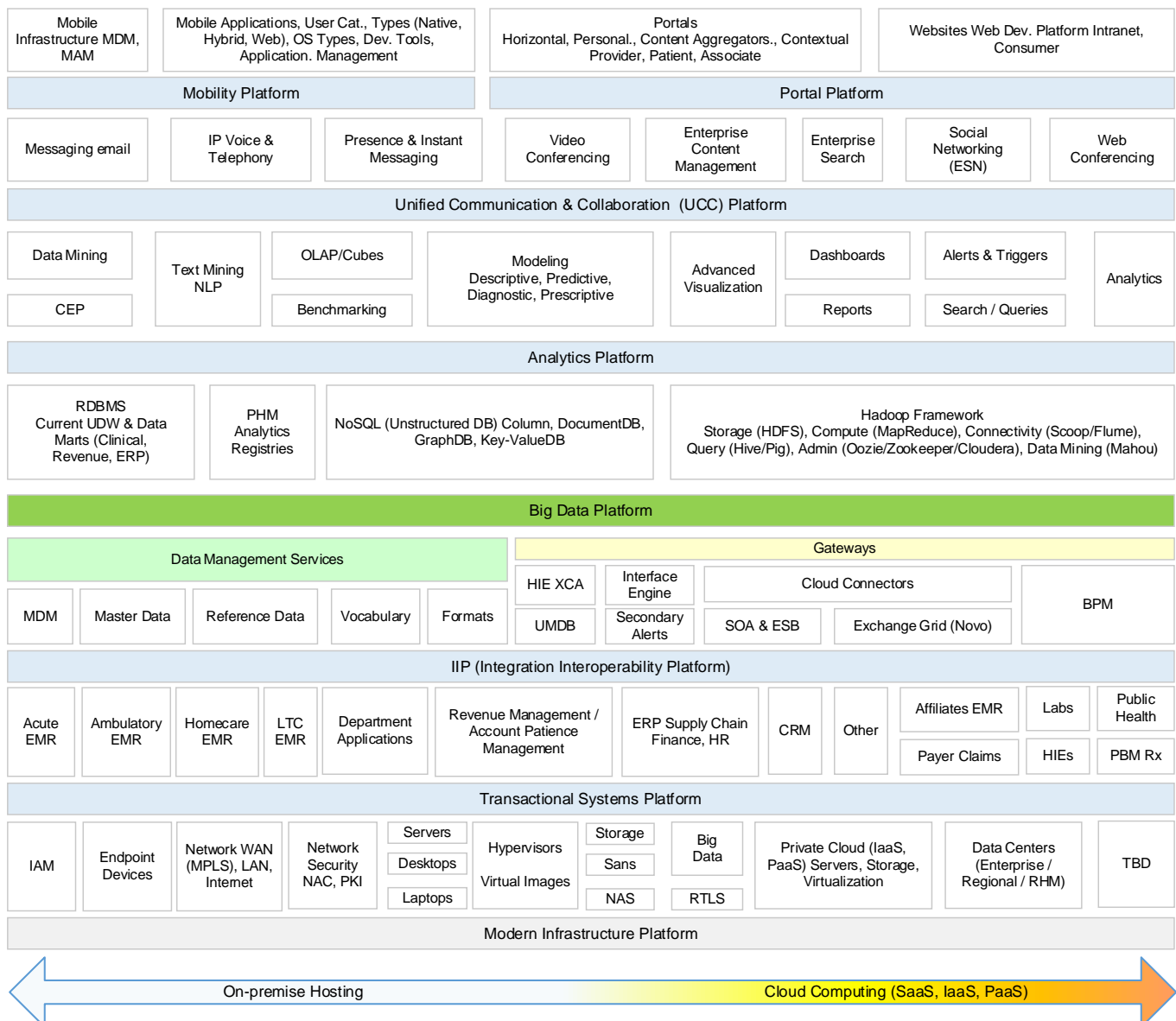
Current ESSO solutions in the enterprise include

- Imprivata OneSign
- Caradigm Vergence

Next Steps

- Approve NetIQ as the Web SSO enterprise standard
- Finalize and Execute Roadmap. – Owner: Technology Services
 - Identify the applications that should use SSO.
 - Develop support model for both Web SSO and ESSO.
 - Select ESSO solution(s).
 - Deploy ID Federation (preferred) or WAM, for Web applications.
 - Deploy ESSO, for non-web applications and shared workstations.
 - Approved NetIQ as the Web SSO enterprise standard
 - Finalize and execute the roadmap as presented

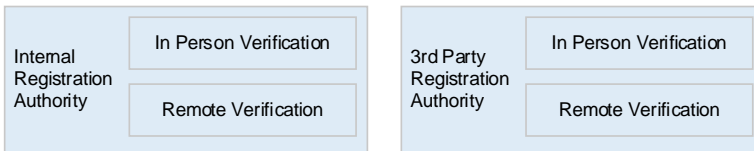
Governance, ITSM, Financial Stewardship, Talent Management



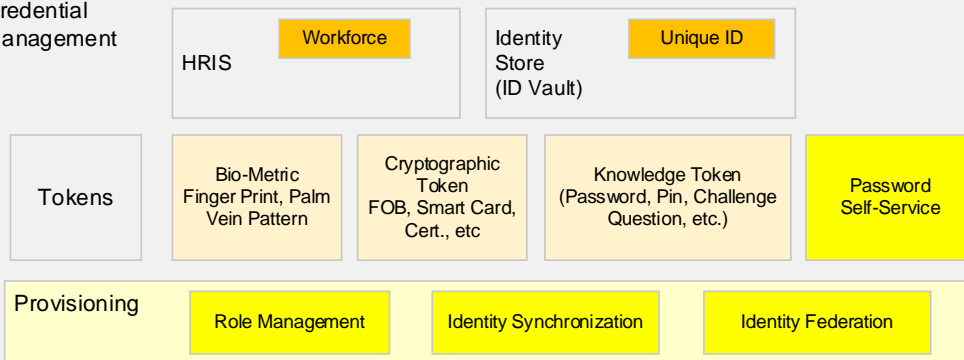
IAM Conceptual Model

Identity and Access Management (Credential Service Provider)

Identity Proofing

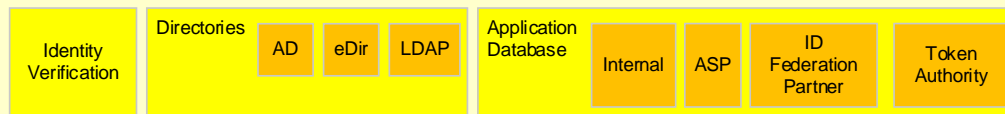


Credential Management



Access Management (Relying / Service Provider)

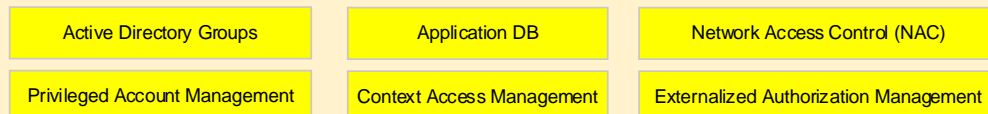
Authentication



Single Sign-on



Authorization



Identity Administration & Governance (IAG)

Identity Auditing

Entitlement Administration

Access Certification

Role Management

Access Request

Access Policy Management

SSO Model Comparison

Solution	Benefits	Limitations and Risks
1. WAM	<ul style="list-style-type: none"> Enables single sign-on for web applications. Mature solution. Greatest reach. Interface with apps can happen quickly. Does not require a trust relationship. 	<ul style="list-style-type: none"> Doesn't enable Corporate to be the IDP for ASPs. Doesn't support automated user account creation and deletion. Only works with web applications. Limited internal support experience.
2. Identity Federation (Preferred)	<ul style="list-style-type: none"> Enables Corporate to be the Identity Provider for ASPs. Improves ability to enforce Corporate IAM and IAG Policies. Access to web apps is disabled as soon as the user's IDP account is disabled. Enables single sign-on for web applications. Enables sharing of identities across trust domains. 	<ul style="list-style-type: none"> Only works with web applications. Not all web applications support federation for authentication. Limited internal support experience.
3. ESSO	<ul style="list-style-type: none"> Eliminates repetitive login by users. Enables shared Workstation requirements (screen locking, time-outs, Biometric access, Proximity access, Security Badge access, etc). Eliminates the need to remember multiple passwords. Reduce risk of compromising all accounts by maintaining different passwords on every system. Utilize strong password rules across apps. Supports both internal and external systems. 	<ul style="list-style-type: none"> Requires named user licenses. Requires deployment of client software to every device. Requires maintenance of custom scripts by application. Relies on technology (e.g. Operating System specific), which may not be available across multiple types of devices. Enabling self-service password management requires additional software. Compromise of the SSO password enables access to all other applications.

Resolution Center Password Resets

Application	Password Reset Issues	% of password resets
PeopleSoft	1	23.69%
Cerner	9	17.55%
Novell Login	3	5.59%
HealthStream	2	4.23%
HealthQuest Patient Management (PM)	2	4.00%
Tel- Trouble Voicemail password	2	3.57%
PeopleSoft Benefits Administration	1	3.33%
GroupWise	1	2.20%
Password Self Service	1	2.16%
Microsoft Outlook	1	2.14%
PeopleSoft Payroll	1	2.14%
Kronos Timekeeper	1	1.80%
Active Directory	9	1.77%
PeopleSoft eApps	9	1.75%
User App	9	1.63%
Vista Plus	8	1.48%
Windows 7	7	1.40%
RegAssist	5	0.97%
HEAT Self Service	5	0.89%
Psynch	4	0.82%
Vision-Security	4	0.79%
TransSpec	4	0.76%
PeopleSoft Human Resources	4	0.75%
Claims Administrator	4	0.72%
Novell Secure Login	2	0.53%
Vision-Clinical	2	0.49%
Nightingale	2	0.48%
EasyAccess	2	0.47%
TSO	2	0.47%
NextGen EPM	2	0.46%
Total		90%

Imprivata OneSign Shared Workstation Features

- In many clinical areas, users do not have the time to logout out of Windows and then back in as a new user. Many users share a group of workstations and need to be able to quickly and securely move in and out of them.
- OneSign can be install in a 'kiosk mode' that allows for this workflow and still provides Single Sign- On to a user's applications. In kiosk mode:
 - The workstation is logged into windows with a generic account.
 - Users authenticate through Imprivata / AD to simply unlock the workstation. This eliminates the windows login / load time when switching users on a workstation.
 - OneSign has customizable levels of inactivity timeouts, visible-desktop-when-locked (for areas like surgery), and currently-logged-in-user notifications.
 - Importantly, OneSign also provides a 'Single Sign-Out' functionality that closes the

previous user's applications and resets the kiosk for the next user. This can trigger through a timeout or a configurable, single keystroke.

- When required we can still provide users access to their own personal drive mappings, even though they are working on a kiosk workstation.
 - When paired with named-user Citrix connections, Imprivata can drive the roaming of users' Cerner Citrix sessions from workstation to workstation.
- As an available option, users can be given fast workstation access through a variety of mechanisms such as Fingerprint access, Proximity Badge access and "Secure Walk-Away" feature.

Current State Imprivata ESSO Applications List

Applications		
Access MC	Protego (web)	Citrix pragent
Action Pro	Claims Admin	Position Manager
Caradigm Vendor Support	SS iManager	Quickbase
CernerCare	User App	RC Psync login
Cisco Admin	Groupwise Messenger	XenApp
MCHS Admin Cmd Console	Groupwise Webmail	SuccessFactors
MCHS Admin Explorer	Harris Vendor Support	TelAlert
MCHS Admin Regedit	Healthstream eLearning	Change Management
MCHS Admin Task Manager	Heat Self Service	Content Publisher
MCHS Favorites App	Imprivata Vendor Support	Downtime Dashboard
MCHS IE Proxy Login	Jive	Knowledgebase
MCHS Outlook (webmail)	Kronos (web)	Lawson Portal
MCHS Outlook	MCHS Remote XenApp	TIS MyPortal
MCHS Physician Preferences	OneSign Administrator	TAG (Citrix - internal)
SpaceLabs Clinical Access	Outlook Webapp	Citrix Nextgen
Concur (Conlin Travel)	Pathways Admin	Vergence Web Administrator
Diversified Direct	Peers	Webex
Dragon Medical	Peoplesoft	Webex Enterprise
ECM	Peoplesoft RC Password Reset	Zenworks Control Center
Empire Time (Web)	PhoneFactor Admin	

Appendix IV: ESSO Current State

RHM	ESSO		
	Tool	Sample Applications	Workstation types
Campus 1	Imprivata OneSign	Cerner, Kronos, WebEx, ECM, Messenger, Heat, PeopleSoft, Quickbase, Change Mgt, Lawson, My Portal, Jive, other	Shared (kiosk) workstations in clinical areas; single user workstations in Pharmacy and other areas based on need
Campus 2	Imprivata OneSign	Kronos, WebEx, ECM, Messenger, Heat, PeopleSoft, Quickbase, Change Mgt, Lawson, My Portal, Jive	Shared (kiosk) workstations in registration areas.
System Office	Imprivata OneSign	Kronos, WebEx, ECM, Messenger, Heat, PeopleSoft, Quickbase, Change Mgt, Lawson, My Portal, Jive	Colleague workstations
System Office	None	None	None
System Office	None	None	None
System Office	None	None	None

Appendix V: ESSO Current State

E		
Tool	Sample Applications using ESSO	Workstation types
Caradigm Vergence	Meditech Magic, Care Logisitics, GE Muse, Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - non-shared workstations, Clinical shared workstations
Caradigm Vergence	Meditech Magic, Care Logisitics, GE Muse, Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - non-shared workstations, Clinical - shared workstations
Caradigm Vergence	Meditech Magic, Care Logisitics, GE Muse, Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - non-shared workstations, Clinical - shared workstations
Caradigm Vergence	Siemens Physician Portal, Siemens Soarian, Siemens MAK, Allscripts Care Management, Care Logisitics, Forms on Demand, Outlook Web Access, Lawson ESS, Service Desk	Clinical - shared workstations
Caradigm Vergence	Meditech Magic, Care Logisitics, GE Muse, Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - non-shared workstations, Clinical - shared workstations
Caradigm Vergence	Meditech CS, Teletracking Transport, IMBills, Care Evolution HIEBus ("MyHealth Portal"), Outlook Web Access, Service Desk	Clinical - shared workstations
Caradigm Vergence	Meditech CS, FormFast, GE Centricity PACS-IW, PICIS ED PulseCheck, Care Evolution HIEBUs ("My Health Portal"), Siemens Invision, Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - shared workstations
Caradigm Vergence	Meditech CS, FormFast, GE Centricity PACS-IW, PICIS ED PulseCheck, Care Evolution HIEBUs ("My Health Portal"), Siemens Invision, Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - shared workstations

Appendix V: ESSO Current State

ES		
Tool	Applications using ESSO	Workstation types
Caradigm Vergence	Meditech CS, FormFast, GE Centricity PACS-IW, PICIS ED PulseCheck, Care Evolution HIEBUs ("My Health Portal"), Siemens Invision, Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - shared workstations
Caradigm Vergence	Meditech CS, FormFast, GE Centricity PACS-IW, PICIS ED PulseCheck, Care Evolution HIEBUs ("My Health Portal"), Kronos Workforce Timekeeper, Outlook Web Access, Lawson ESS, Service Desk	Clinical - shared workstations
Caradigm Vergence	Meditech CS, Allscripts EHR., Care Logisitics, FormFast, Lawson ESS, Outlook Web Access, Internet Explorer, Service Desk	Clinical - shared workstations
Caradigm Vergence	Meditech CS, Care Logisitics, Outlook Web Access, MediServe Medilinks, Care Evolution HIEBus ("MyHealth Portal"), Allscripts Care Management, Service Desk, PointClickCare	Clinical - shared workstations
Caradigm Vergence	Meditech CS, Care Evolution HIEBus ("MyHealth Portal"), Alpha ImageWorks, GE Muse, PICIS ED PulseCheck, GE Centricity Radiology PACS, Iatrics Mobilab, Outlook Web Access, Lawson ESS, Service Desk	Clinical - shared workstations
Caradigm Vergence	Siemens Physician Portal, Siemens Soarian, NovaRad PACS, GE Muse, Care Evolution HIEBus ("MyHealth Portal"), Outlook Web Access, Lawson ESS	Clinical - shared workstations
Caradigm Vergence	Meditech Magic, GE Centricity PACS-IW, Care Fusion, Outlook Web Access, Lawson ESS	Clinical - shared workstations