SANTA CLARA VALLEY
HEALTH & HOSPITAL SYSTEM

Dedicated to the Health
Of the Whole Community

Mental Health Department

Mental Health Services Act
Capital Facilities and Technological Needs

Enclosure 3 – Exhibit 2
Technological Needs Assessment

May 15, 2009

Enclosure 3
Exhibit 2

Technological Needs Assessment

County Name: Santa Clara

Project Name:

Provide A Technological Needs Assessment Which Addresses Each Of The Following Three Elements

1. **County Technology Strategic Plan Template**
   (Small Counties have the Option to Not Complete this Section.)

   This section includes assessment of the County's current status of technology solutions, its long-term business plan and the long-term technology plan that will define the ability of County Mental Health to achieve an **Integrated Information Systems Infrastructure** over time.

Current Technology Assessment

List below or attach the current technology Systems In Place.

1.1 Systems Overview

SCVHHS MHD utilizes a number of applications to support its day-to-day business operations. In its role as the Local Mental Health Plan, MHD serves as both an administrator of Mental Health services to the County's citizens and as a provider of direct services.

The major applications in use are Uni/Care, Diamond and Invision. Uni/Care is deployed in all of the SCVHHS MHD clinics for capturing service data and billing services. All County clinicians are entering their progress notes into Uni/Care at present. Contract Providers must either directly enter their service data in Uni/Care or submit it electronically.

Diamond is used for the Managed Care Medi-Cal program.

Invision is the client medical record system used by the inpatient psychiatric unit, the psychiatric ER and the Urgent Care Center.

There are a variety of smaller databases, applications, and spreadsheets in use. See Appendix A for an overview of the systems.

List Or Attach A List Of The Hardware And Software Inventory To Support Current Systems.

1.2 Hardware

MHD is part of the County's Wide Area Network and owns application servers, SAN farm, networking equipment and other hardware. See Appendix B for a description of the MHD network, equipment and security standards.

1.3 Software

See 1.1 above. In addition, See Appendix A-2 and Appendix A-3 for an overview of systems.

1.4 Support (i.e., Maintenance and/or Technical Support Agreements)

SCVHHS holds maintenance agreements with all of its hardware and software vendors for support. The maintenance agreements for both Uni/Care and Diamond provide technical assistance when needed.

In addition, SCVHHS IS provides dedicated support staff for the Uni/Care system, Invision and Managed Care Systems (Diamond). MHD staff are able to contact the support staff directly for problems, questions and assistance with reporting needs. See Appendix B-12.

Plan To Achieve An Integrated Information Systems Infrastructure (IISI) To Support MHSA Services

Describe the plan to obtain the technology and resources not currently available in the county to implement and manage the IISI. (Counties may attach their IT Plans or complete the categories below.)

1.5 Describe how your Technological Needs Projects associated with the Integrated Information System Infrastructure will accomplish the goals of the County MHSA Three-Year Plan.

The TN Projects associated with the IISI are the Electronic Health Record (EHR), Enterprise Data Warehouse (EDW), County Health Record Initiative (CHR), and Bed and Housing Exchange Database Project (BHX).

All of these projects will improve the County's ability to coordinate care for their clients as well as support their recovery in the community.

Electronic Health Records will streamline the clinic visit, eliminate the use of paper charts, eliminate the shuffling of paper charts between providers, allow multiple providers to see a complete treatment picture, eliminate the completion of redundant client forms, and provide tools to better monitor a client's recovery.

The Enterprise Data Warehouse will consolidate data from all systems into a single repository and make it easier for staff to generate meaningful management reports, detect effective treatment protocols, monitor client progress, and identify candidates for FSP programs and intensive case management. In addition, the Data Warehouse will serve as the integration tool for all systems and client data useful to MHD for efficient management of its programs. Data mining tools and end user reporting tools will enable staff to track, monitor and report program outcomes.

A County-wide Health Record and Master Patient Index (MPI) will enable coordination of services across agencies. This information will enable staff to better support consumers in the community. The information will also provide staff with timely information about children at risk who present for services at multiple agencies.

The Bed and Housing Information Tracking database will assist staff and consumers with identifying housing opportunities in the community and track availability of beds for consumers requiring urgent or emergent care.

See the IT Roadmap document in Appendix C-5 for a diagram of how the components of these projects relate to the IISI.

1.6 Describe the new technology system(s) required to achieve an Integrated Information System Infrastructure.

All projects will use existing technology and adhere to hardware, software, security and architecture standards currently in use at SCVHHS MHD. The following applications described in the Enclosure 3 documents will provide new functionality for MHD.

1. Electronic Health Record. MHD records consumer progress notes into their current EHR, Uni/Care. This project will expand the functionality to meet full EHR standards and mandates. This will include online assessments, treatment plans, workflow capability and create a paperless treatment environment.

2. Enterprise Data Warehouse. This project will require new software tools that have not been used by MHD and IS staff at Santa Clara County. This component is where full data integration of client data will occur. Extract, transform and load tools will be implemented. The mapping of the data and the creation of data standards will be new to Santa Clara MHD.

3. Personal Health Records. The EHR software will enable SCVHHS MHD to offer their clients PHRs. The methodology and products will be determined as part of the project.

4. Computerized Physician Order Entry, including e-RX. This will allow psychiatrists and other treatment staff to issue a prescription or lab order, send it electronically to the pharmacy or lab and obtain the lab results electronically.

5. Consumer and Provider Portals. These secure applications utilize web-based portal technology. Portal technology will be new to MHD staff. This project will enable consumers and providers to conduct business with MHD online.

6. Interoperability. SCVHHS is not currently sending data to anyone except the State DMH. The technology and mechanics of exchanging client data securely will be detailed during the project planning and design phases of the County Health Record Initiative.

1.7 - Note the Implementation Resources Currently Available.

Oversight Committee:	◉ Yes	○ No
Project Manager	◉ Yes	○ No
Budget:	◉ Yes	○ No
Implementation Staff in Place:	◉ Yes	○ No
Project Priorities Determined:	◉ Yes	○ No

1.8 - Describe Plan To Complete Resources Marked “No” Above.

Existing staff will be totally involved in the implementation process. It will be necessary to augment existing staff with contract resources from the chosen vendor and other sources. The temporary staff will include technical resources, operational resources, data entry resources and other resources to support normal clinic operations during the training and implementation phases of the project. See the Electronic Health Record Exhibits 3 and 4 for additional detail regarding staffing.

1.9 - Describe the Technological Needs Project priorities and their relationship to supporting the MHSA Programs in the County.

MHD priorities are serving its clients and supporting their clients to live in the least restrictive environment possible. The MHSA recovery model supports wrap around services that facilitate independent living and integration into the community. The TN projects listed above in 1.6 all contribute and support those goals by providing technology tools to facilitate care coordination, monitor outcomes, and identify clients needing more intense services before reaching a point where extended residential care is required.

The Exhibit 3 documents for each project discuss the project relationship to MHSA programs and IISI infrastructure.

2. Technological Needs Roadmap Template

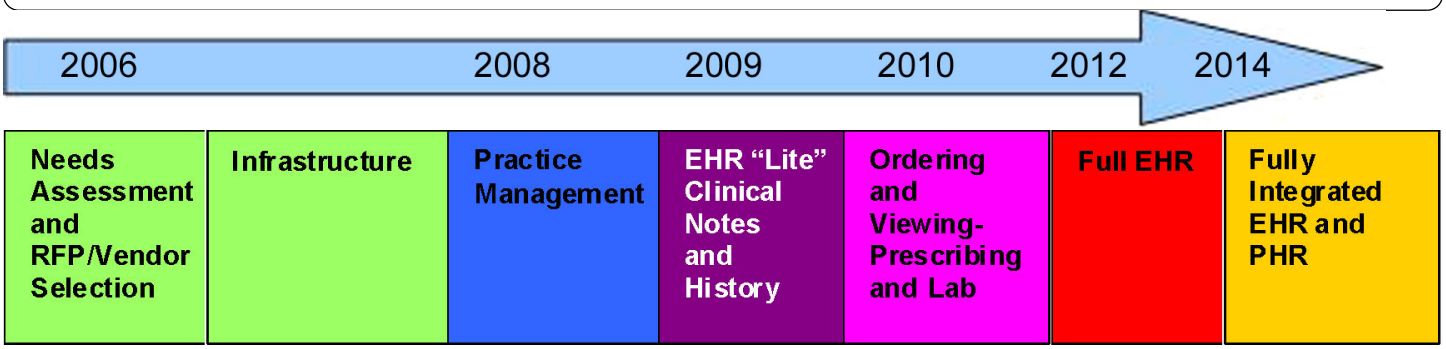
This section includes a Plan, Schedule, and Approach to achieving an Integrated Information Systems Infrastructure. This Roadmap reflects the County's overall technological needs.

Complete a Proposed Implementation Timeline with the Following Major Milestones.

2.1 List Integrated Information Systems Infrastructure Implementation Plan and Schedule or Attach a Current Roadmap (example below).

See IT Roadmap document in Appendix C-5.

2.2: See Training Guidelines in Appendix B and Training Schedule in Appendix C.



2.2 Training and Schedule (List or provide in Timeline Format…Example Below)

Training Schedule for 2008	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Basic System Nav	X											
Admin Staff	X											
Clinicians		X										
Contract Providers		X										
Client Look-up			X									

2.3 Describe your communication approach to the Integrated Information Infrastructure with Stakeholders (i.e., Clients and Family Members, Clinicians, and Contract Providers).

In order to develop the MHSA TN Request, Santa Clara conducted an IT Assessment and Gap Analysis. The Gap Analysis helped identify potential projects for consideration. For a description of the Assessment process see Appendix C.

See Exhibit 5 documents in the Enclosure 3 documents for each TN Project for a list of the meetings held to discuss these projects.

In addition to these meetings, training and communication plans will be developed for each of the projects during the project planning phase. There will be formal and informal verbal and written communication to the stakeholders as implementation of EHRs and PHRs occurs.

2.4 Inventory of Current Systems (May include System Overview provided in County Technology Strategic Plan).

See Appendix A.

2.5 Please attach your Work Flow Assessment Plan and provide Schedule and List of Staff and Consultants Identified (May complete during the Implementation of the Project or RFP).

The Workflow Assessment Plan will be developed as part of the Electronic Health Record Project during the project planning phase. It is envisioned that Contractors will be solicited to assist with the workflow assessment and that this activity will be done in conjunction with the selected vendor as functionality is phased into production. The steps to the plan will include:

1. Identify key processes
2. Form workgroups of key staff to develop current workflows
3. Facilitate workgroups and capture current procedures
4. Validate accuracy of workflow documentation
5. Analyze the workflows and identify opportunities for improvement
6. Review opportunities and workflows with staff
7. Create standard procedures for common and often repeated processes
8. Post and distribute to staff for review and comments
9. Review workflows with vendor and adjust to system constraints as necessary
10. Revise workflows and procedures
11. Train staff on new procedures
12. Implement new procedures.

2.6 Proposed EHR component purchases [May include information on Project Proposal(s)].

See EHR Enclosure 3 for more information.
SCVHHS MHD will assess their current system (Uni/Care) to see if it can continue to meet its needs. If they decide to continue with Uni/Care they will implement the full-functionality offered by Uni/Care and expand their current system to a full-functioning EHR.

If they decide that Uni/Care is not appropriate for their future environment, MHD will purchase another full EHR product via an RFP process that meets County procurement rules.

In either case, MHD is seeking a single, integrated product to meets its EHR needs.

2.7 Vendor Selection Criteria (Such as Request for Proposal).

If MHD remains on the Uni/Care platform, MHD and IS will work together with the vendor to implement the remaining modules / functions to bring their installation up to a full-functioning EHR and offer a paperless environment. MHD has a contract with Uni/Care and a new amendment to the current contract will be negotiated.

If MHD chooses to purchase a new product they would have to issue an RFP that meets County Procurement rules.

2.8 Cost Estimates associated with achieving the Integrated Information Systems Infrastructure.

EHR: $13.6 million
EDW: $ 2.6 million
CHR: $ 1.1 million
BHX: $ .2 million

Total: $17.5 million

See Enclosure 3 Exhibit 4 Budget Summaries for each project for more information.

NOTE: Santa Clara County received approval on their Enclosure 1 Component Proposal for over $13 million for its MHSA Technological Needs (35% Capital / 65% Technology Split). Subsequent to submitting that request a Technological Needs Assessment was completed and detailed planning on the seven MHSA IT projects began. During the planning process, Santa Clara County realized that the Technology Projects must be properly funded to ensure success and a significant factor to the successful implementation of an Electronic Health Record will be transitioning the Contract Provider agencies to an EDI environment. As noted in the Component Proposal, the stakeholder process overwhelmingly supported technology solutions. As the Budget Summaries were completed for the Technology Projects Santa Clara County realized the need to increase the amount of money allocated for technology projects to nearly $18 million. This will change the Capital Facilities / Technology Projects Split to 15% / 85%. These additional technology funds will be used primarily to support the Contract Provider agencies as they transition to the EHR environment.

3. County Personnel Analysis (Management and Staffing)

- All **Authorized # FTE Authorized** staff will not be paid out of MHSA funds.
- All **Estimated #FTE Needed in addition to #FTE Authorized** staff will be funded with MHSA funds.
- 2.5 FTE of the **Project Managerial and Supervisory** staff will be funded with MHSA funds:
  1. .5 Project Lead
  2. .5 Health Education Coordinator (Project Lead)
  3. Consumer Skills Coach (Project Lead)
- The Clinical Project Director, Project Manger and one Project Lead will be authorized to the projects 100% but will not be funded with MHSA funds.

Major Information Technology Positions	Estimated # FTE Authorized	Hard to Fill? 1 = Yes 0 = N	Estimated #FTE Needed in addition to #FTE Authorized
A. Information Technology Staff (Direct Services)			
System Administration		1	1
Interoperability Analyst		1	1
DBA		1	1
Programmer / Data Modeler		1	2
Subtotal A		4	5
B. Project Managerial and Supervisory			
CEO	1		
MHD County Director	1		
CIO	1		
MHD Deputy Director	1		
MHD Division Director	1		
Clinical Project Director	1		
Project Manager	1		
Project Leads	1	1	.5
Health Education Coordinator (Project Lead)			.5
Consumer Skills Coach (Project Lead)			1
Subtotal B	8	1	2
C. Technology Support Staff			
Training		1	1
Data Quality Assurance		1	2
Clerical / Administrative		1	1
Data / Interface Monitoring		1	1
Financial – Billing Support and Budget Analyst		1	3
Consumer Peer Support		1	2
Subtotal C		6	10
Total County Technology Workforce (A+ B + C)			
			17

Appendix A: Current Systems – Overview

Guide to Appendix A Documents

Appendix A-1: Overview & Description
Appendix A-2: SCVHHS MHD Systems Diagram
Appendix A-3: SCVHHS MHD Systems Functions Chart
Appendix A-4: SCVHHS MHD Provider Information Systems Model

Systems Overview

SCVHHS MHD accesses a number of applications to support its day-to-day business operations. In its role as the Local Mental Health Plan, MHD serves as both an administrator of MH Systems overseeing eligibility, service authorization, provider claims payment and billing. MHD is also a provider of direct services and operates nine MH clinics.

The major applications in use are UniCare, Diamond and Invision. UniCare is deployed in all of the SCVHHS MHD and DADS clinics for capturing service data and billing those services. Contract Providers must either directly enter their service data into UniCare or submit it electronically.

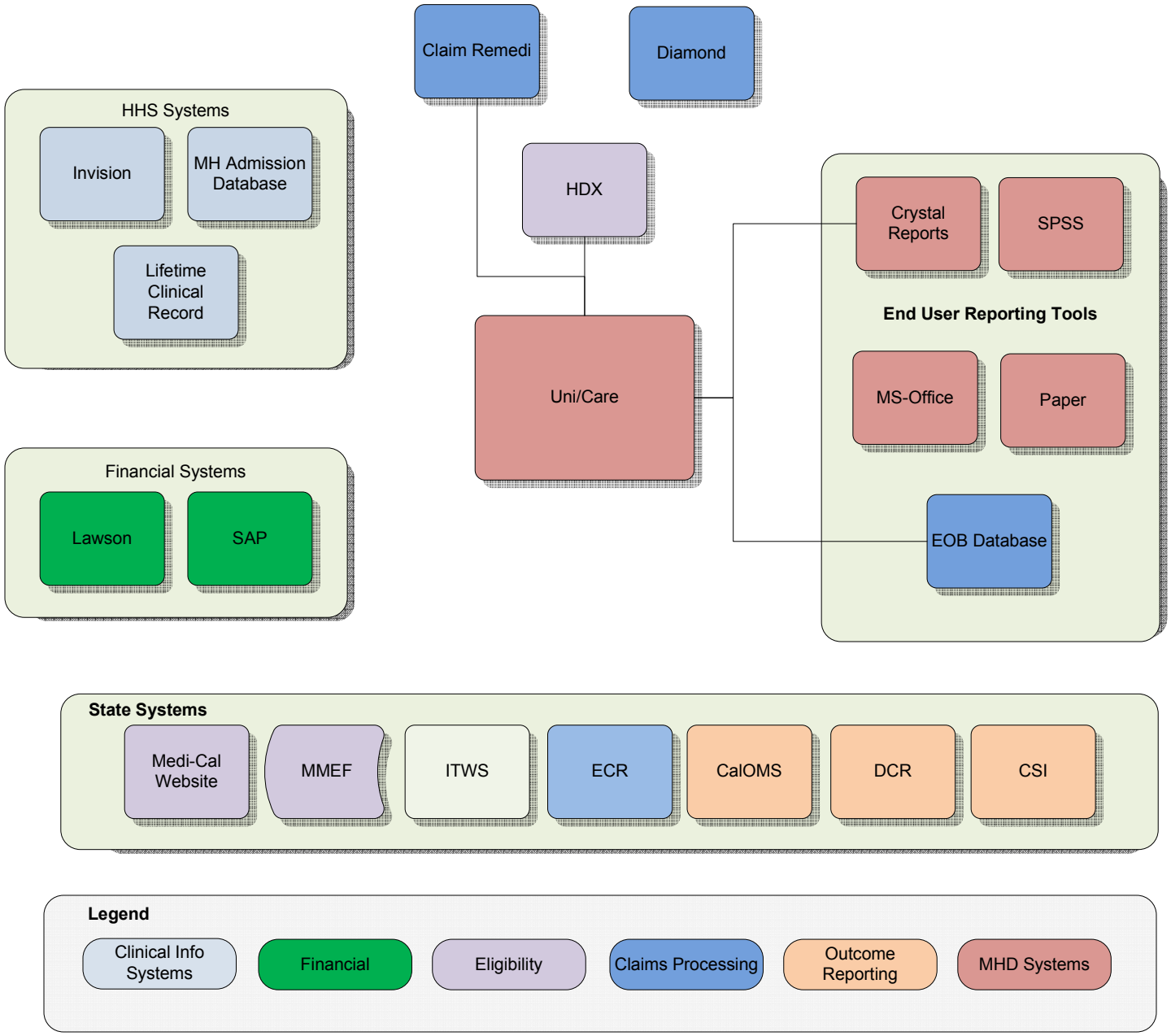
Diamond is used for Managed Care Medi-Cal program.

Invision is the Valley Medical Center system used by the inpatient psychiatric unit, the psychiatric emergency room and the Urgent Care Center.

The following table lists the major applications in use by MHD with a brief description of their functionality.

SCVHHS Developed & Maintained Applications	
Admissions Database	Database of hospital admissions
EOB Database	Locally developed database that contains Medi-Cal EOB data
Lifetime Clinical Record	Interface to HHS Lifetime Clinical Record that provides information on medications and lab results for clients that use Valley Medical Center.
Outsourced Applications	
Claim Remedi	Claims clearinghouse
COTS Applications	
Crystal Reports	End-user Reporting Tool
Diamond	Managed Care System for FFS Medi-Cal
HDX	Eligibility and Insurance look-ups
Invision	Hospital system; client registration info
Lawson	Financial System used by HHS
MS-Office Suite	Documents, spreadsheets, calendars
SAP	County financial system and enterprise resource system
SPSS	Statistical and reporting tool
Uni/Care	Main application to record client services
State DMH Applications	
CalOMS	Treatment data compliance standards for CA Dept. of Alcohol and Drug Programs
DCR	CA DMH System to collect outcomes data for MHSA FSP programs
ECR	CA DMH System for correcting pended claims
ITWS	CA DMH site for uploading and downloading files
Medi-Cal Website	System used for checking Medi-Cal eligibility online
CSI	CA DMH System to collect FSP Program data

SCVHHS Current State Diagram



5/13/09

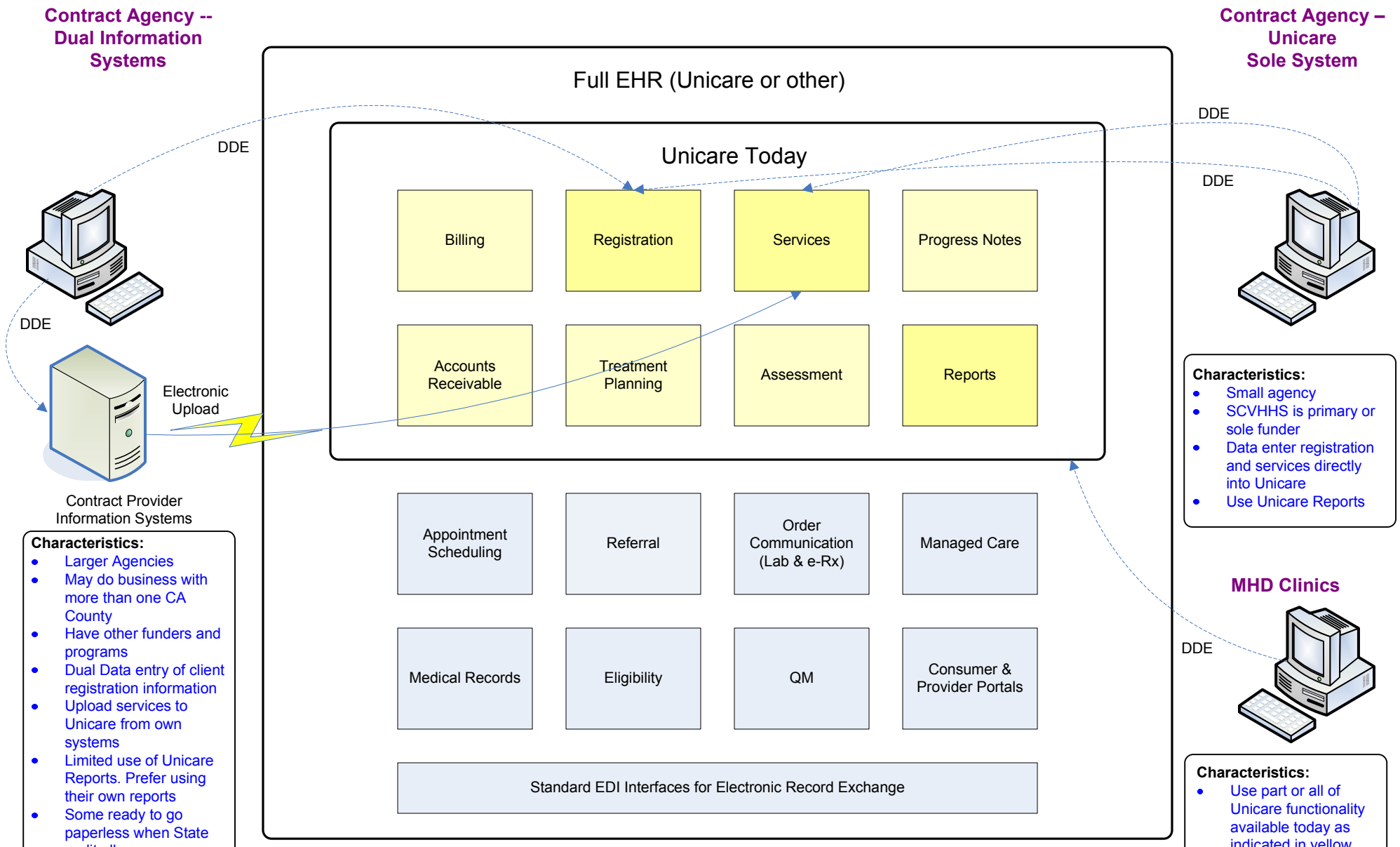
SCVHHS MHD
Systems and Functions Chart

Appendix A-3

✓ Currently using

Functions		Systems and Tools																			
		COTS Applications								Homegrown Applications			External	State DMH Tools						Personal Electronic Files	Paper
		Uni/Care	Diamond	Invision	HDX	SPSS	Lawson	SAP	Crystal	LCR	EOB Database	Admissions Database	Claim Remedi	M/Cal	ITWS	ECR	CalOMS	DCR	CSI	MS-Office	Paper
MHD Providers	Contact Tracking / Screening	✓																		✓	✓
	Client Registration	✓	✓	✓																	
	Assessment Management	✓																			✓
	Financial/ Benefits Determination		✓		✓									✓							
	Appointment Scheduling																			✓	✓
	Tx/Care Plan Management																				✓
	Progress Note Management	✓								✓										✓	✓
	Order Communication									✓											✓
	Service Capture	✓	✓	✓								✓								✓	✓
	Billing and A/R Management	✓	✓	✓			✓	✓			✓	✓	✓		✓					✓	
	Summary Health Record	✓								✓											
	Case Load Management	✓										✓								✓	✓
MHD Administration	Call Center Tracking	✓																			✓
	Referral Tracking	✓																			✓
	Eligibility Management				✓									✓							
	Credentialing	✓	✓	✓																	✓
	Contracting																			✓	✓
	Authorization Management		✓									✓								✓	
	Claims Adminstration	✓	✓	✓							✓	✓	✓		✓	✓				✓	
	Financial Management						✓	✓							✓						
	Outcome Measures	✓													✓		✓	✓	✓	✓	✓
	Reporting	✓	✓	✓		✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓

SCVHHS MHD
Provider Information Systems Model



NOTE:
- Functionality to be added for Full EHR capability will require increased data entry requirements.
- All FSP providers must enter DCR data directly into State system

Appendix B: Current Systems – Infrastructure

Guide to Appendix B Documents

Appendix B-1:	Overview
Appendix B-2:	SCVHHS MHD Servers and LAN Schematic
Appendix B-3:	SCVHHS MHD Uni/Care Network
Appendix B-4:	SCVHHS MHD Technical Standards
Appendix B-5:	SCVHHS Network Management Policy
Appendix B-6:	SCVHHS Data Backup Plan
Appendix B-7:	SCVHHS Business Continuity Plan (Table of Contents)
Appendix B-8:	SCVHHS IT Security Policies
Appendix B-9:	SCVHHS Business Associate Agreement
Appendix B-10:	SCVHHS IT Training Methodology
Appendix B-11:	SCVHHS Training Materials and Delivery Methods
Appendix B-12:	SCVHHS MH and DADS Support Summary

Infrastructure Overview

Mental Health Department (MHD) systems are hosted in a data center operated by Santa Clara County Health and Human Services (SCVHHS). This data center is a state of the art facility that hosts systems for several County Departments other than Mental Health. The County manages the networking equipment, power, temperature controls, and other aspects managed by County data center staff. Currently the County's policy is to own, not lease, hardware equipment and refresh equipment on a 5 year cycle.

SCVHHS has a standardized, open architecture enterprise system operating under multiple platforms with Windows as the primary platform. Additional platforms include UNIX, AIX and Open VMS. The Windows platform is an Active Directory Schema with replication amongst County ISD, SCVHHS and CISD sites. Each of these sites serve as a backup to each other for authentication of any user within the SCCGOV.ORG domain. Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Windows Internet Naming Service (WINS) are also supported.

New server platform is based on blade server technology connected to SAN with redundant Gb fiber connections.

IP address assignment is handled through redundant DHCP servers operating on Microsoft Windows 2003 servers, which also support DNS, roaming user profiles, and central administration, distribution, and enforcement of desktop configuration.

Management of the network servers is under the direction of Enterprise Server Management Group (ESMG). They are responsible for the building, design and implementation of domains, support of operating systems and maintenance of over 250 servers that house enterprise applications such as e-mail, SQL, Oracle, Citrix and departmental applications such as Uni/Care, as well as personal and shared folders.

ESMG uses Netbackup and Tivoli Storage Manager as the enterprise archiving / backup system to ensure data integrity and prevent data loss. Symantec AntiVirus Corporate Edition is used to protect the enterprise from computer virus attacks, spyware and adware.

SCVHHS has a standardized computer platform that consists of personal computer (PC) hardware, desktop operating system, office application suite and e-mail. The computer platform is reviewed annually and revised to keep up with technology changes.

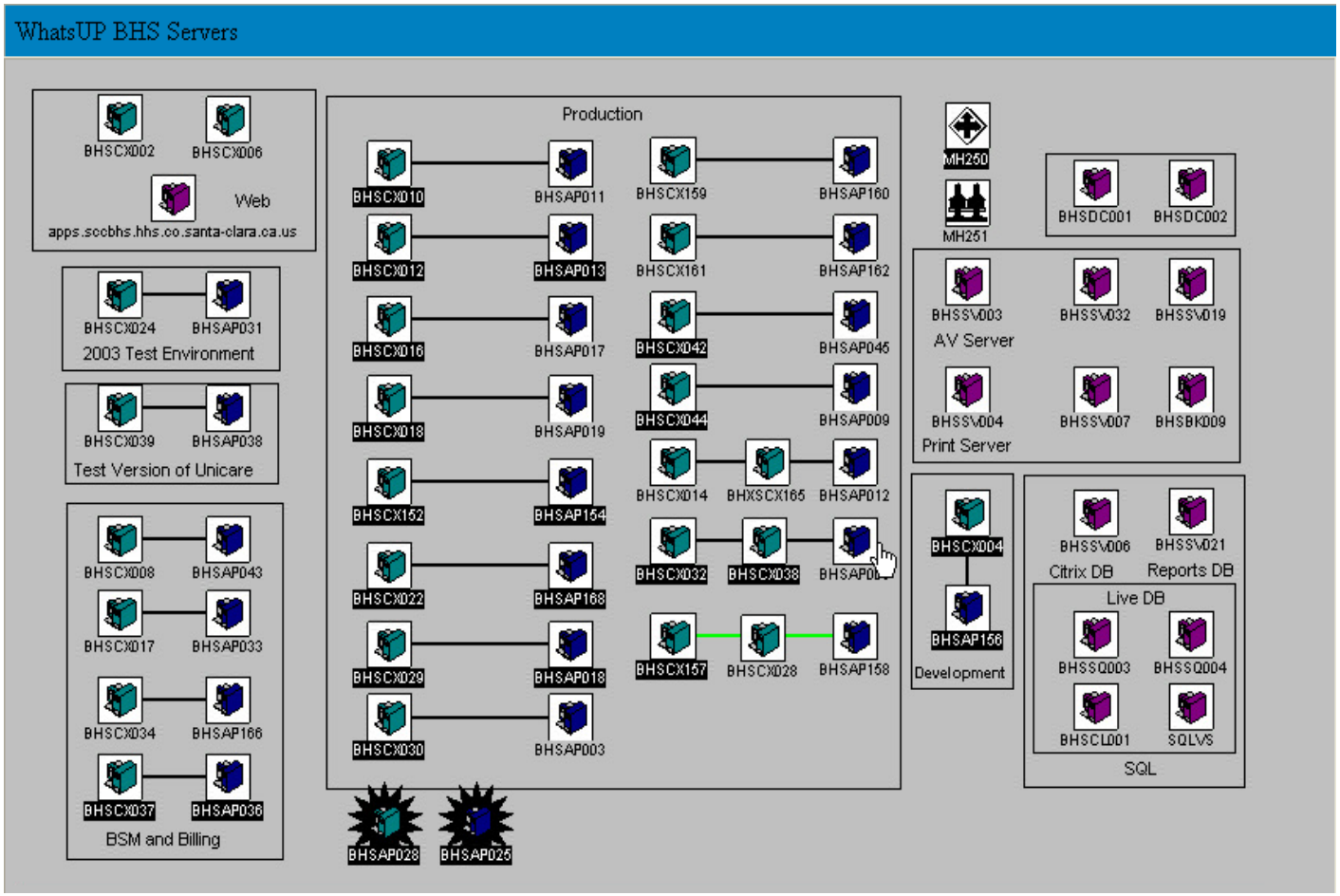
The core of the SCVHHS network consists of a redundant fiber optics backbone powered by a series of Cisco routers. SCVHHS is standardized on Cisco infrastructure. SCVHHS also employs VLAN technology. There are fiber links to 20 campus buildings. Remote sites, including clinics, are linked via dual redundant T-1 lines and Metro Ethernet.

SCVHHS has developed a complete set of policies to protect the data and network, ensure smooth operations, guard against loss of data and provide quick recovery in case of network failure or disruption. The security policies meet HIPAA standards for PHI and industry IT standards. Copies of these policies are contained within this Appendix for review. Please note that only the Table of Contents has been provided for the Business Continuity Plan. The complete document is very lengthy. The Table of Contents provides a good overview of its contents. Detail on any part of that plan can be provided upon request.

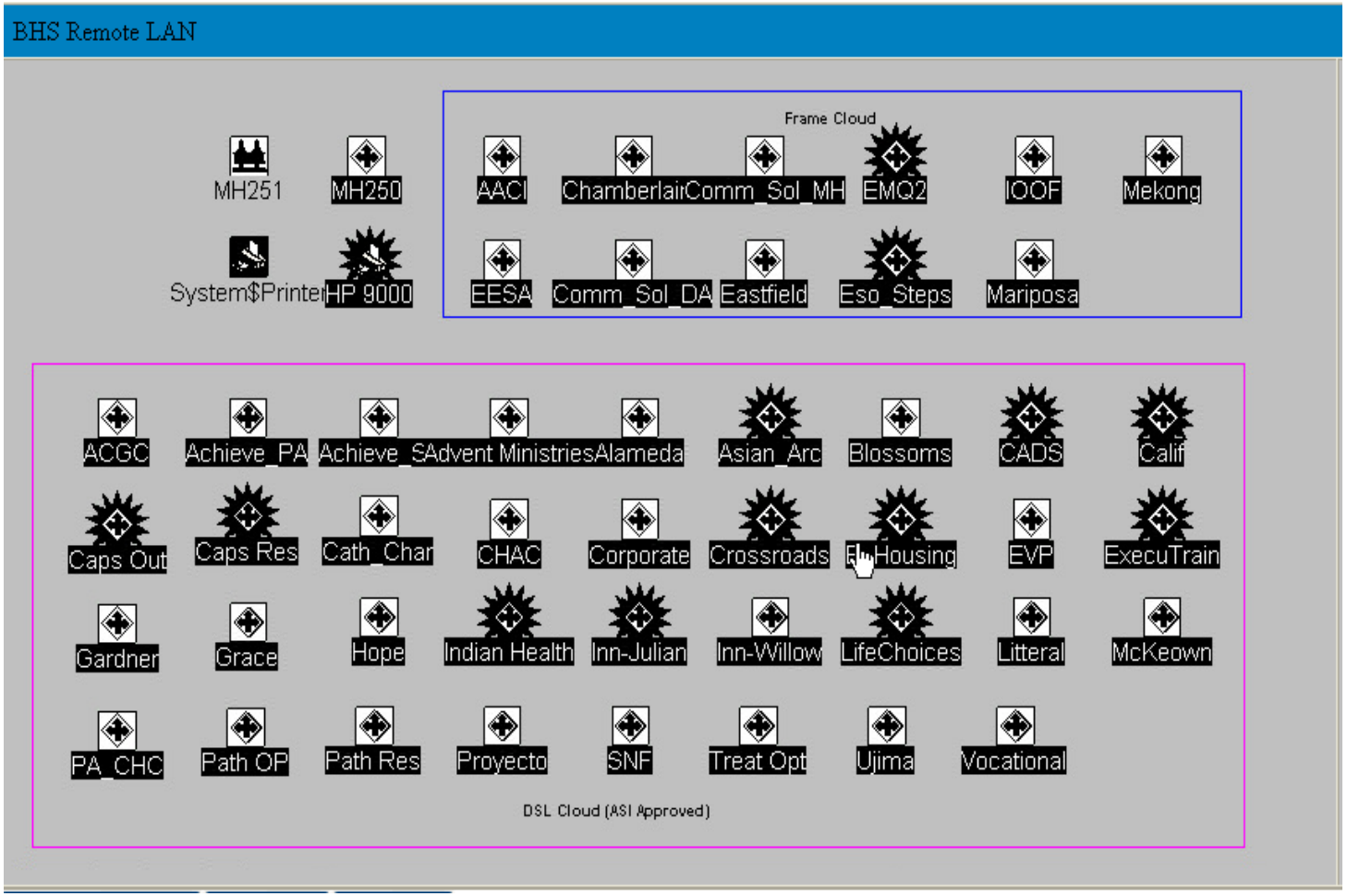
Finally, SCVHHS has developed two documents regarding training guidelines for all major systems that they support. These documents have been included as well.

SCVHHS MHD Server and LAN Schematic

Server Configuration

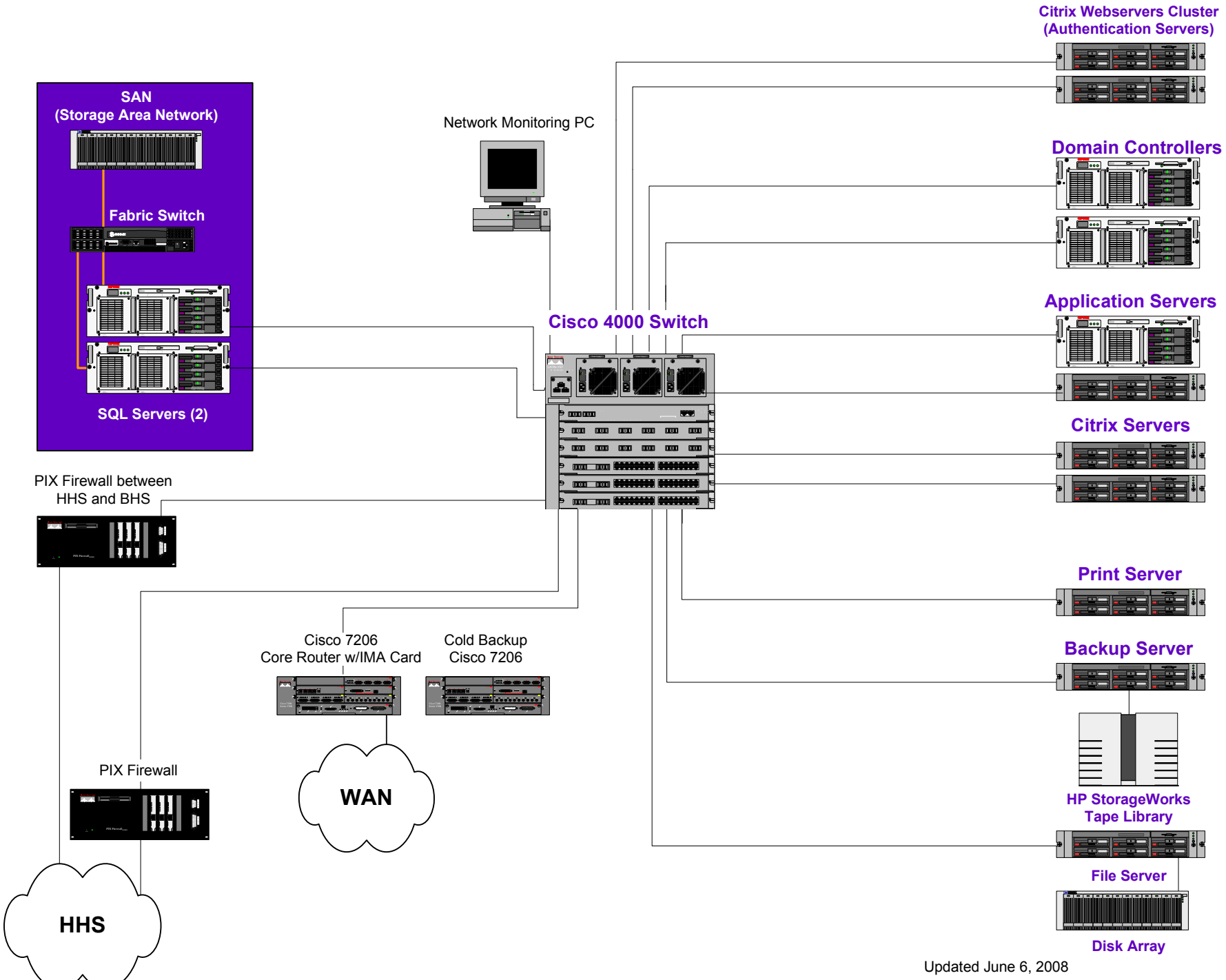


LAN Configuration



SCVHHS MHD Uni/Care Network

Appendix B-3



Updated June 6, 2008

Santa Clara Valley Health and Hospital System
Information Services – Technical Services
Technical Standards – Intel Platform

2/23/07

SERVER

Operating system	Windows Server 2003/Windows Active Directory
Hardware	Intel Dual Core 3.0 GHZ – 2MB cache, fiber/GBE NIC (redundant), SAN integration via Emulex 1000-L2 HBAs, dual processor, 2GB RAM per processor minimum, redundant power supplies. Blade technology preferred.
Backup	Veritas NetBackup 4.x and/or Tivoli Storage Manager *(enterprise backup)*
Server redundancy/cluster	Depends on application
Disk array	Raid 1(Blade),Standalone: RAID 1 (OS) RAID 5 (Data)

DESKTOP/LAPTOP HARDWARE

Mid-level PC with 17" monitor	HP DC7700 Convertible Mini-tower For most current spec see Valley Pages – Forms – Information Services – HHS Special Specifications
Small footprint PC with flat 17" LCD panel monitor *(where space limitations require small footprint)*	HP Ultra-Slim Desktop – DC7700 For most current spec, see Valley Pages – Forms – Information Services – HHS Special Specifications
Monitor settings	1024 x 768/ high color
Laptop	HP NC8430 – 15.4" display, Wi-Fi a/b/g For most current spec see Valley Pages – Forms – Information Services – HHS Special Specifications
Docking station	Basic docking station 1.1

DESKTOP/LAPTOP SOFTWARE

Operating System	Windows XP with Service Pack 2
Office applications	Microsoft Office 2003 Professional, SP2
Email	Microsoft Outlook 2003
Terminal emulation	NetManage Rumba 2000 v.6
PDF reader	Adobe Acrobat Reader 7.0
Desktop database	Microsoft Access 2003
Internet browser	Microsoft Internet Explorer 6.0
Antivirus	Symantec AntiVirus Corporate Edition Version 10.x
Java	Java Version 1.4.x
Encryption – ***Laptop Only***	PointSec v6.1

PRINTERS

Laser	HP LaserJet – Group - Mid-range printer is 4250TN HP LaserJet – MFP is HP 4345TN HP LaserJet – standalone is HP2105D
Impact	Not supported
Label	Zebra with network connectivity
Network interface	HP- Internal Jet Direct

COMMUNICATION

Protocol	TCP/IP
Topology	Ethernet
Routers/ switches	Cisco
Bandwidth – network	Gigabit (sx/lx)
Bandwidth – to the desktop	10/100 MB/ second
Backbone	Fiber optic
Cable to the desktop	Category 5e UTP with RJ45 connections

REMOTE AUTHENTICATION/SUPPORT

CRYPTOcard via Cisco VPN

SANTA CLARA VALLEY HEALTH & HOSPITAL SYSTEM

Administrative Policies and Procedures

Central Services Policies and Procedures

February 6, 2006

TO: SCVHHS Executive Management Group

FROM: Kim Roberts
Acting Executive Director, SCVHHS

SUBJECT: **Network Management**

POLICY:

Santa Clara Valley Health and Hospital System (HHS) Information Services Department (IS) is responsi8ble for designing, planning and coordinating the development of the HHS enterprise computer network (HHS Network) which includes departmental local area networks (LAN) and wide-area networks (WAN). The development of a coordinated HHS enterprise network promotes connectivity between departments and systems, reduces costs, increases productivity, and provides a focal point for support.

IS establishes standards for networks, communications connectivity protocols, personal computers, end-user devices, services, information systems architecture, software, peripherals, security, and E-mail. Any exceptions to standards must be approved by IS.

IS provides or coordinates design, upgrades, maintenance and support for the HHS Network. IS sets policy and standards for management of the HHS Network.

IS develops an annual budget for network infrastructure equipment and network cabling projects. Departments are responsible for budgeting for departmental infrastructure, servers, software and additional devices except as by agreement between the Department and IS.

NETWORK MODIFICATION PROCEDURE:

Responsible Party	**Action**
Department Manager or Designee	Network modifications may be requested by Department Managers, typically at the level of Cost Center/ Nurse Manager, Site Manager, Program Manager, Department Chair/ Chief or above - or by manager's designee. Submits a written request (Device Activation Request and/ or scope of work and/ or project description) to IS.
Information Services	Open Case and reviews request. If necessary, advises Department on technical standards and/or security issues. Coordinates consultation and/or approval process with County Information Services Department if necessary.

Approves or denies request. Assists as appropriate with implementation.

New projects which require technology with significant complexity or security concerns may require review and approval by the Information Systems Steering Committee through the Project Evaluation and Prioritization (PEP) process.

Attachment: Device Activation Request

Issued: 05/19/2003
Revised: 02/06/2006

NETWORK SERVICES
Santa Clara Valley Health & Hospital System
2325 Enborg Lane, Suite 1K104
San Jose, CA 95128
Tel: 408.885.5300 Fax: 408.885.5380

SCVHHS NETWORK DEVICE ACTIVATION / RELOCATION REQUEST

TACOPs Case # HD: _____

Submitted by: _____ **Phone:** _____ **Date:** _____

DAR Type:

☐ Add PC new install ☐ Remove PC from network recover IP: _____

☐ Project Location: _____

☐ Edit:

☐ Move From: _____ To: _____

☐ MAC edit Old MAC: _____

☐ PC Replacement (Complete old PC information for replacement device)

Serial Number: _____

Asset Number: _____

MAC Address: _____

PC new install image: ☐ **W2K** ☐ **XP** PC Re-image: **W2K** ☐ ☐ **XP**

HHS Image version #: _____ PC Image / Re-Image Date: _____

Comments: _____

Device / Location Information

Device Type: ☐ PC ☐ Printer ☐ Other _____

Current Device ID: _____ MAC Address: _____

Asset #: _____ Serial #: _____

End User / Responsible: _____ Phone: _____

Department: _____

Location: Building: _____ Floor: _____ Room/Cube: _____

PC Hardware:

PC Type: **Processor:** **Memory:**

Printer Hardware:

Printer Type: Invision Printer? LU #

Network Information (For IS-Technical Services Use Only)

New Device ID: _____ VLAN _____ Type of Install: ☐ DHCP ☐ Hardcoded

IP Address: _____ Subnet Mask: _____ Gateway _____

Initial & date box when complete

IP BOOK ☐ **DHCP** ☐ **IPDB** ☐

DAR V2005 (Rev: 07/22/05)

February 2005

TO: SCVHHS Executive Management Group

FROM: Robert Sillen
Executive Director, SCVHHS

SUBJECT: **DATA BACKUP PLAN**
45 CFR § 164.308(a)(7)(i)(A)

STANDARD: **CONTINGENCY PLAN**

See HHS Appendix A for definitions used throughout this document.

POLICY:

Data Backup Plan – Each HIPAA impacted County agency/department will establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI) held by the covered entity.

This policy is to be reviewed annually to determine if the policy complies with current HIPAA Security regulations, in the event that significant related regulatory changes occur, or in response to environmental or operational changes affecting the security of ePHI.

PROCEDURE:
HIPAA-impacted Agencies/Departments must apply the following procedures to all information systems that contain or use ePHI.

14.3.1 Implement Backup Procedures

All Departments must develop formal procedures for backing up critical system configuration files, databases, and end user data files.

14.3.1a – Backup Mission-Critical Databases and Data Files

All mission-critical databases and data files must be included in the Department backup procedures.

14.3.1b - Backup All Critical System Files

System configuration files should be included in the backup process since they are difficult to reconstruct. System files should be backed up before all system changes, as well as after every system change, but only after testing has verified that the changes have been implemented correctly.

14.3.1c – Do Not Over-Write Most Recent Previous Backup Version

Backups should never be done as an over-write of the most recent, previous backup version; at least one previous backup must be maintained at all times. In addition, several generations of backups should be saved in case of major problems, or in case a critical file is lost. The number of generations of backups that should be retained depends on the individual Department business environment. The recommendation is that at least one year's worth of backups for critical databases should be maintained.

14.3.1d - Automate the Backup Process

The backup process should be automated as much as possible, and a specific schedule for performing these backups should be established, published, and followed.

14.3.1e - Maintain "Emergency Kits"

For all servers, the master boot record information should be backed up and placed on an "emergency rescue" floppy disk or CD that is stored in a locked cabinet. Installation kits and documentation for all installed software should be maintained in a centralized area, since in many cases comparison of these original files with current files is the only way that changes made to the system by an intruder can be detected.

14.3.2 Establish Frequency and Extent of Backups According to Business Needs

Both the frequency and extent of system and database backups will vary from Department to Department, and should be based on the criticality of individual systems and applications. For critical applications, databases might require hourly backups, while non-critical databases might not require more than a once-a-week backup. Backup frequency and extent must be in accordance with the importance of the data and an acceptable level of risk.

14.3.3 Make Provisions for Backing Up User Files

If data is backed up only on servers and not on client (user) machines, a dedicated server, directory, shared drive, or other designated location must be designated where Users can store critical data files for automated backup. Departments should make sure that Users know how to send their critical files to these areas, and a schedule of the automated backup process should be published so that Users know when these backups occur. Users should be instructed to move their critical files to this backup area on a regular basis.

14.3.5 Select a Safe, Secure Location for Storing Backup Media

Departments must ensure that the location selected for storing backup media is both secure and protected from environmental hazards such as water pipes.

14.3.5a - Ensure Physical Security of Storage Location

Departments must ensure that the physical security of designated backup storage locations is commensurate with the level of sensitivity and/or confidentiality of the data. Physical access to the backup media must be controlled according to the same requirements as the source systems.

14.3.5b – Limit Access to Only Authorized Individuals

Individual access to backup media should be commensurate with the classification level of the data, and only authorized individuals should have access. If backup media are stored in off-site, third-party vendor facilities, the vendor's employees must be bonded, and subject to the same background checks as County employees would need to be permitted access to the data.

14.3.6 Label Backup Media

At a minimum, all tapes and other backup media must be labeled with information that identifies the data, the date of data (backup) creation, and the data classification label. More complete identifying information is recommended, which includes, but is not limited to, the following:

- System/Application Name
- Agency/Department Contact Information
- Purge Date

14.3.7 Test the Backup Process

The success of the backup process must be verified in some manner. For example, this might involve verifying that the directory structures and files sizes on the backup media match the directory structures and files sizes on the operational system.

14.3.8 Test the Restoration Process

At least once per year, Departments should practice performing restorations from backup media in non-emergency situations to ensure that the process is understood, and also to ensure that the restoration process itself is working correctly. Testing of the restoration process should include both restoring individual files and complete database/system restoration.

15.3.4d – Long-Term Storage Standards

LONG-TERM STORAGE STANDARDS			
Public	***Internal***	***Confidential***	***Restricted***
No special precautions required for any media type. ***(Note: Electronic storage media includes Video, CDs, Floppies, DVDs, hard drives, etc.)***	**Printed materials:** Reasonable precautions to prevent access by non-employees. **Electronic documents:** Storage on all drives permitted. **Email:** Reasonable precautions to prevent access by non-employees. **Electronic storage media:** No special precautions required	**Printed materials:** Store in secure manner (e.g., secure area, lockable enclosure). **Electronic documents:** Storage on secure drives only. Storage on shared drives without password protection for reading is prohibited. **Email:** Must be stored in a secure manner, e.g. password access or reduce to hard-copy form, delete electronic form, and store as for Confidential printed materials. **Electronic storage media:** All media must be labeled with classification information.	**Printed materials:** Store in secure manner (e.g., secure area, lockable enclosure). **Electronic documents:** Storage on secure drives only. Password protection of each *document* encouraged. Encryption recommended. **Email:** Must use one of following: 1) Reduce to hard-copy form, delete original message, and store as for Restricted printed material. 2) Archive with password protection and delete original message. Encryption recommended. **Electronic storage media:** Media must be labeled with classification information. Must be locked up when not in use. Control sheet required (with signature and date) for removal from locked storage.

15.3.4e – Labeling Standards

LABELING STANDARDS			
Public	***Internal***	***Confidential***	***Restricted***
Labeling not required for any media.	**Paper Documents**: All documents must be labeled with the classification on the first page or cover. **Electronic Media:** Labeling not required.	**Paper Documents**: For paper documents, each page must be labeled "Confidential." **Electronic Media:** Media must be labeled "Confidential."	**Paper Documents:** For paper documents, each page must be labeled "Restricted." Individual copies must be labeled with a unique identifier (e.g., "Copy 1 of 10"). **Electronic Media:** Media must be labeled "Restricted." Individual copies must contain a unique identifier.

16.3.4b – Evaluate Backup Policy

The ASP must have a policy for backing up all databases and critical system files that is consistent with the importance of the application. Backup media must be treated according to the level of security of the data they contain.

18.3.3b – Establish User Guidelines For Retaining/Archiving Business Electronic Records

Users should be provided with guidelines for the process of retaining/archiving Business Electronic Records. Users should also be provided with a procedure for transferring email messages that should be retained on a more permanent basis (i.e., Business Electronic Records) to a location that has been designated for this purpose, such as a special server, an archival folder, or shared drive.

Users must also be instructed on how to classify and label Business Electronic Records and email messages that are to be saved/archived according to content, the Department's classification scheme, and the established records retention schedule.

Responsible Parties:

Reference and/or Related Policies:
45 CFR §164.308(a)(7)(i) – Contingency Plan (Standard)
County IT Security Policy 14, 15, 16, 18
JCAHO IM.2.10, 2.20, 2.30, 6.60

Issued: MM/DD/YY
Date Revised: MM/DD/YY

SCVHHS Business Continuity Plan
Table of Contents

COUNTY OF SANTA CLARA

INFORMATION TECHNOLOGY SECURITY POLICIES
(Abridged Version)

May 15, 2008

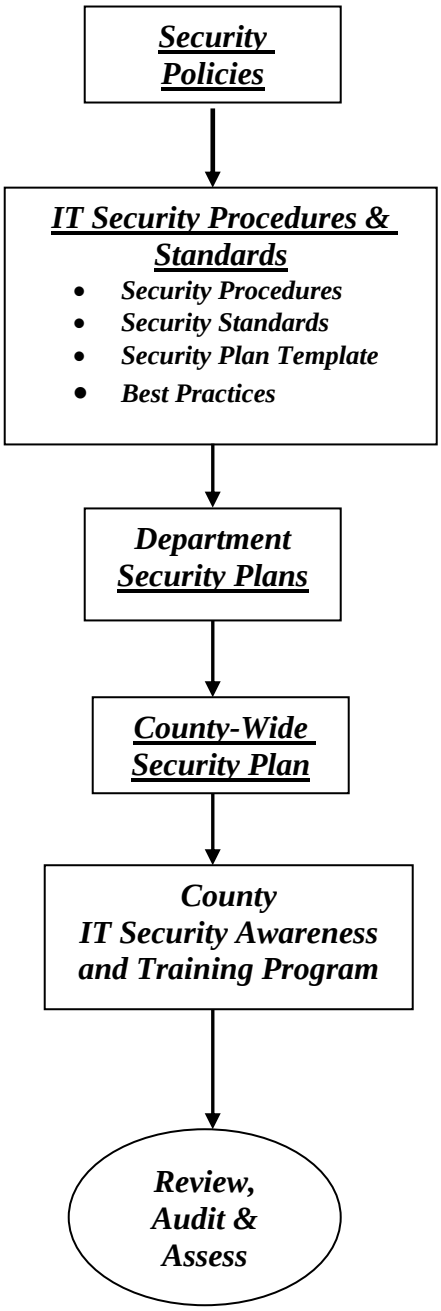
TABLE OF CONTENTS

1.0 COUNTY INFORMATION TECHNOLOGY SECURITY PROGRAM

The Board of Supervisor's resolution of June 25, 2002 authorized the County's CIO to develop a comprehensive security program. Under the sponsorship of the CIO, senior IT managers from several County Agencies were invited to participate as members of the Information Security Development Group (ISDG). This group is responsible for developing and updating the County's IT security policies, procedures and standards, and for providing recommendations regarding IT security to the County CIO.

The following diagram illustrates the process used to define and implement the County's information security program.

COUNTY INFORMATION SECURITY PROGRAM PROCESS



2.0 ABRIDGED INFORMATION TECHNOLOGY SECURITY POLICIES

The full version of the *IT Security Policies* defines a common environment within the County that fosters system security, ensures data integrity and privacy, and prevents unauthorized access, misuse, damage to, or loss of County IT assets and/or data. This document provides an abridged version of the policies and should be used only as a general reference and guide to the full policies.

3.0 GENERAL SECURITY POLICIES

The General Security Policies provide the foundation for all other County IT Security Policies, as well as for all associated security standards, procedures, and best practices.

- All information created or used within the County in support of County business activities is considered to be the property of the County, and must be protected during its useful life until authorized disposal.
- Each Agency shall operate in a manner that is consistent with maintaining a common, shared, trusted computing environment within the County.
- Each County Department shall prepare and implement an annual *IT Security Plan*, as well as participate in periodic, County-wide security assessments conducted by an independent third party.
- Each County Department shall correct any significant deficiencies identified in its *IT Security Plan,* and/or during the County-wide security assessment.
- Each Agency shall ensure that all Users receive appropriate training in IT security.
- All Users must read and acknowledged all required statements, forms or other documents related to IT security and/or access to County information and data.
- Each Agency, and all County employees, shall adhere to all restrictions in the use of software programs as specified in the relevant software licensing agreements.

4.0 LOCAL USER LOGON AND AUTHENTICATION

This policy describes the requirements associated with authenticating Users who attempt to access County owned computer resources <u>from within the County network infrastructure</u>.

- Departments shall establish a procedure that ensures only Users with legitimate needs to access County IT resources are provided with user accounts.
- No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs.
- The level of authorization assigned to individual User accounts shall be restricted to those privileges required to support legitimate County business processes.
- At logon, the User shall be presented with a statement ("login banner") containing language on appropriate use of County computer systems.
- All access to County computer systems shall be controlled by a minimum of a User Identifier (ID) and password combination.
- Users of County computer resources are prohibited from sharing either their user account or password with others.
- County approved standards shall be used in constructing passwords.
- Auditing and logging of User activity shall be implemented on all critical County systems.

5.0 INTERNET USE

The purpose of this policy is to define the basic principles for employee and Department business use of the County's Internet access infrastructure.

- No Department shall implement its own connection to the Internet without prior written approval from the County CIO.
- Transmitting any electronic communication over the Internet that contains Confidential or Restricted information is prohibited, except under the conditions specified in Policy 15.0, Data Classification.
- No County employee, contractor, or consultant shall use the County's Internet infrastructure for inappropriate purposes.
- All Department servers that are accessible from the Internet shall be protected by a security infrastructure approved by the County CIO, and shall be configured to minimize security vulnerabilities ("hardened").
- County employees are prohibited from utilizing, participating in, or configuring Internet-based Instant Messaging (IM) services. If needed to support legitimate business processes, a Department may use an internal, County-provided instant messaging service.
- County employees are prohibited from utilizing, participating in, or configuring Internet-based Peer-to-Peer or file sharing services.

- Employees are prohibited from participating in Internet discussion groups unless there is a legitimate business need to do so, and explicit permission has been given by Department management.

6.0 EMAIL

This policy addresses appropriate use of Internet and County email systems.

- No employee, contractor or consultant shall use County-owned email systems for inappropriate purposes.
- Each User of a County email system shall have an individual email account. Users shall not use the email account assigned to another individual to either send or receive messages.
- Use of Internet (external) email systems is prohibited unless there is a compelling business reason for such use.
- When used, the interface with an Internet (external) email system must be configured such that email messages are inspected for malicious software.
- Users shall not configure or use automated forwarding of County email messages to Internet (external) email systems unless specifically authorized to do so.
- Attachments to email shall be governed by all procedures and standards related to the classification level of the data.
- County-approved language, informing recipients how to handle the message, must be appended to all email messages sent from County email systems.
- Features designed to filter out malicious software contained in email messages and attachments shall be implemented on all County email systems.
- Business-related email messages on County email systems that are no longer necessary shall be routinely deleted.
- Users shall not delete email messages whose subject matter is relevant to pending or anticipated litigation or other legal processes.
- Departments shall formulate a policy on the use of encryption with email messages that is consistent with other County policies regarding data privacy and confidentiality.
- Other than mechanisms specifically authorized by a Department, use of user-set passwords or other message locking/protection measures (such as encryption) are prohibited on County email systems.

- Departments shall provide employees with training on the appropriate use of Internet and County email systems, and on handling email messages and attachments.

7.0 MALICIOUS SOFTWARE

The intent of this policy is to minimize the incidence and impact of computer viruses, worms and other forms of malicious software ("malware").

- Users of County networks and computer resources shall not knowingly create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.
- Anti-virus software shall be installed, configured, and maintained in an active state on each County-owned computer system. The anti-virus software shall be regularly updated to ensure that the anti-virus signatures are maintained in a current state.
- Other measures as prescribed by County-approved procedures and standards, such as maintaining computing devices at current operating system patch levels, shall be followed to minimize the potential impact of malicious software.

8.0 REMOTE ACCESS

The intent of this policy is to ensure secure access to County IT assets from non-County facilities.

- The common County-owned network infrastructure shall be used for remote access to County IT assets.
- Remote access implementations involving technology, designs, or configurations not previously deployed within the County shall be subject to a detailed design review and subsequent certification by the County CIO's Office.
- Remote access in which file systems or applications are accessed shall use a minimum of two-factor authentication.
- Session inactivity time-outs shall be employed for all remote access into and from County networks.
- All remote access infrastructures must include the capability to monitor and record a detailed audit trail of each remote access attempt, including date, session start and end times, and User ID.

- Users are prohibited from connecting and/or activating dial-up modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.
- Each Department shall conduct regular internal audits to identify unauthorized, active modems; unauthorized modems identified during these audits shall be disabled immediately.
- All devices that are used for remote access shall be configured with current operating system security patches, current anti-virus software, approved firewall software, and/or other specified security products.
- Any computing device that has been disconnected from a County network, and subsequently used to connect to a non-County infrastructure, shall NOT be re-connected to a County network until the device has been verified to be free from viruses and other forms of malicious software.
- All laptops and other portable devices brought into County facilities shall be evaluated for compliance with County standards regarding anti-virus software, operating system patch levels, and other security measures and products. Devices that do not comply with the standards shall not be connected to County networks until the appropriate security features have been implemented.
- Remote access privileges shall be granted to County employees only for legitimate business needs.
- Remote access privileges shall not be given to third parties unless the relevant Department head determines that these individuals have a legitimate business need for such access.
- Third-party remote access shall be limited to those privileges and conditions required for the performance of the specified work.
- Users granted access to the County's IT infrastructure using remote access mechanisms must follow all additional policies, procedures and standards related to authentication and authorization on local (internal) County systems.

9.0 PHYSICAL ACCESS

This policy is designed to ensure that all County organizations have deployed suitable physical access controls.

- Mainframes, servers, and network computing devices (such as routers and switches) shall be placed in a location where physical access is limited to authorized individuals.

- In County facilities, network connectivity by unauthorized individuals shall be prevented by limiting access to network cabling and in-wall data ports.
- Unauthorized disclosure of Confidential or Restricted information contained on devices such as printers, fax machines, and computer hard drives shall be prevented by appropriate physical controls.
- All County employees, and authorized contractors/consultants and vendors, shall wear a valid County identification badge when working in a County facility.
- Temporary guests to any non-public County facility or area shall sign in and be provided with a Visitor's badge, which is to be worn while in the facility or area.
- Guests in County facilities shall be escorted by a County employee when in areas that contain restricted information and/or mission-critical servers or network equipment.

10.0 COMPUTER SECURITY INCIDENT RESPONSE

This policy describes the procedures to be used by each Department in planning for, and responding to, computer security incidents.

- Each Department shall participate in the County's security incident response program.
- Each Department shall designate one individual as its Security Liaison, and at least one additional individual as a back up to the Security Liaison.
- Each Department shall designate a primary and a back up point-of-contact that can be reached after normal work hours in the event of a security incident.
- Each Department shall prepare a written Incident Response Plan that includes procedures for recognizing, managing, documenting, and escalating security incidents.
- Departments shall respond to security advisory information by promptly undertaking appropriate and/or recommended procedures intended to mitigate the effects of actual or potential security incidents.
- The Security Liaison shall notify other County organizations of all real or suspected security incidents that occur within the Department, even if the incident has apparently been dealt with successfully.

11.0 DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

The purpose of this policy is to ensure that each County organization has developed internal plans for continuing business operations in the event of a disaster.

- Each Department shall develop a Disaster Recovery Plan, as well as a Business Continuity Plan (BCP).
- Safeguards shall exist within each Department to minimize the risk, cost, and duration of disruption to business processes in the event of damage to, failure of, loss of, corruption of, or discontinuation of a strategic component of the critical infrastructure.
- Each Department must provide for re-establishing critical and essential systems and applications that may have been disrupted due to an unforeseen event.

12.0 CHANGE CONTROL

This policy is intended to ensure that essential hardware and software are protected against unauthorized changes that could cause systems to malfunction or fail.

- Users shall not make changes to system and/or software configuration files on County computer systems.
- Users shall not download and/or install operating system software or other software applications, including computer games, on County computer systems without prior written authorization.
- Each Department shall develop a Change Control Procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT infrastructure.
- Each Department shall conduct periodic audits designed to determine if unauthorized software has been installed on its computers.

13.0 DATA ENCRYPTION

The purpose of this policy is to ensure the privacy and confidentiality of passwords and other sensitive information during both transmission and storage.

- Encryption shall be used to protect files and/or email messages containing Confidential or Restricted data that are transmitted over open, untrusted networks, such as the Internet.

- Only County-approved encryption technologies shall be used for encrypting files and/or email messages.
- Encryption keys shall be exchanged using secure methods of communication.
- Departments shall optionally encrypt stored data files in order to protect Confidential or Restricted data.
- Departments shall optionally encrypt stored email messages in order to protect Confidential or Restricted data.
- Confidential and Restricted data that is stored on any mobile device shall be encrypted.

14.0 BACKUP

The purpose of this policy is to establish minimum requirements for the backup and storage of critical application databases and system configuration files.

- Each Department shall implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations.
- The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk.
- A server, shared drive, directory, or other location shall be designated where Users can send critical data files that are to be included in the backup process.
- Departments shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards.
- Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.
- Departments shall define and test a formal procedure designed to verify the success of the backup process.
- Restoration from backups shall be tested at least once per year to ensure that databases and system configuration files are recoverable.

15.0 DATA CLASSIFICATION POLICY

The purpose of this policy is to provide guidelines for identifying and protecting sensitive information.

- Each County organization shall identify all essential business-related data that are owned, used, or generated within its environment that can be classified as Confidential or Restricted.
- All data that has been identified as specified above shall be assigned to an "owner" within the organization.
- Data that has been identified as either Confidential or Restricted shall be consistently protected from its origination through its destruction.
- Access to Confidential or Restricted data shall be limited to properly authorized individuals, and such data should only be accessed for legitimate business needs.
- Contracts that involve sharing data identified as Confidential or Restricted with other entities shall include language designed to ensure that this information is used solely for contractual purposes, and is not shared with, transferred to, or sold to unauthorized third parties.
- Information repositories potentially accessible to the general public shall not store data identified as Confidential or Restricted without appropriate, well-established, industry-standard safeguards.
- County organizations receiving information from other organizations shall classify and handle it according to County policies.

16.0 APPLICATION SERVICE PROVIDER (ASP)

The purpose of this policy is to ensure that ASPs selected to host County applications are held to the same security standards as internal County organizations.

- Departments shall evaluate all existing ASP implementations for consistency with County policies and standards, and shall prepare a remediation plan for those implementations that do not meet these policies and standards.
- Security standards for planned ASP-hosted applications shall be evaluated and certified by the County CIO.
- ASPs used by County Departments shall be required to have a Business Continuity Plan (BCP) and/or a Disaster Recovery Plan (DRP).
- ASPs used by County Departments shall be required to have a formal, published IT Security Policy that addresses how it manages and maintains the internal security posture of its own infrastructure.

17.0 WIRELESS COMMUNICATION

The purpose of this policy is to define the standards for deployment and use of wireless technology within the County.

- Only wireless systems that have been evaluated and certified for security shall be approved for connectivity to County networks. All access to County networks or computing resources via unapproved, wireless communication technologies is prohibited.
- All approved wireless systems implemented between or within County facilities shall follow all standards for securing wireless systems.
- County data that is transmitted over any wireless network must be protected according to the classification of the data.
- Each Department shall make a "best effort" to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environment.
- Any unauthorized wireless modems and/or access points shall be disabled immediately.

18.0 ELECTRONIC RECORDS RETENTION

The purpose of this policy is to provide County organizations with general guidelines for the responsible management, retention and deletion/archival of business-related electronic records.

- Departments shall maintain the integrity and availability of Business Electronic Records while the records still have business value, or for as long as required by law and/or Department policy.
- Department management shall develop a retention schedule indicating the length of time that Business Electronic Records are to be retained before these records are subject to destruction.
- Department management shall establish guidelines for retaining and deleting Business Electronic Records, and shall ensure that Users are aware of these guidelines.
- Informational Electronic Records shall be deleted when their administrative business purpose has been served.
- Personal Electronic Records (e.g., personal email messages) shall be promptly deleted once such records have been read.

19.0 APPLICATION SECURITY

This policy describes the requirements associated with securing County business applications.

- Departments shall identify all business applications that are used by the Department in support of its primary business functions.
- An Application Owner shall be designated for each primary Department business application.
- Departments shall establish procedures that ensure only Users with legitimate needs to do so have access to primary business applications.
- Access controls associated with Business Applications shall be commensurate with the highest classification of data used within the application.
- If access to an application is password-based, at a minimum the standards for password generation and use must comply with all standards specified in Section 4.0, Local User Authentication and Authorization.
- A business application user account shall be explicitly assigned to a single, named individual. No group or shared accounts are permissible except when necessary and warranted due to legitimate business needs.
- User privileges associated with business applications shall be commensurate with the highest level of data used within the application. The level of authorization shall also be restricted to the minimum privileges required for the user to perform a specified job function.
- Auditing and logging of end user activity shall be implemented on all critical County applications.
- Security requirements shall be incorporated into the evaluation process for all commercial software products and/or Business Tools that are intended to be used as the basis for a Business Application.
- All County IT security policies, requirements, and standards shall be incorporated into the design and implementation of new business applications.
- A combination of technical, procedural and physical safeguards shall be used to protect application code from unintentional or unauthorized modification.
- A formal Configuration Management Plan shall be required prior to the implementation and subsequent maintenance of any new mission-critical software application.

20.0 ADMINISTRATIVE PRIVILEGE MANAGEMENT

This policy describes the requirements associated with managing the enhanced privileges delegated to those individuals responsible for administration and maintenance of County computer systems.

- Departments shall establish a procedure that ensures only authorized individuals (i.e., "Administrators") are provided with enhanced system privileges.
- The privileges assigned to Administrators shall be restricted to those required by the individual to perform necessary administrative and maintenance tasks (principle of "least privilege").
- The use of specialized Administrative accounts shall be limited to those circumstances in which system administration and management tasks cannot be performed using standard User accounts with enhanced privileges.
- County standards for constructing, distributing, and managing passwords used for authentication to accounts with enhanced privileges shall be applied to all administrative and maintenance access to County systems.
- Procedures shall be established to ensure that administrative passwords are protected from disclosure to unauthorized individuals.
- Auditing and logging of privileged system commands shall be implemented on all servers and other County infrastructure systems that support this feature.

21.0 MOBILE DEVICES

This policy describes the requirements for the use, configuration, management, and disposal of mobile devices used for County business purposes.

- Unless there is a legitimate business reason for doing otherwise, all mobile devices used to access County resources, and/or to process or store County data shall be selected from the list of devices approved for use within the County.
- Employees shall utilize County-provided mobile devices for work-related purposes only. Employees are prohibited from allowing individuals who are not County employees from utilizing the device for any purpose.
- All mobile devices shall be required to successfully authenticate at the designated, approved County network point-of-entry prior to being granted access to any County network, resource, application, or data.

- Approved methods for preventing the introduction of malicious software must be implemented on all mobile devices that are used to access County networks, information technology resources, applications, or data.
- Appropriate controls shall be implemented on all mobile devices such that the confidentiality of data on the device is protected.
- All networking and connectivity features on mobile devices that are not required in support of County business applications shall be disabled.
- Appropriate measures shall be taken to ensure that mobile devices are protected against loss or theft.
- Departments shall define and implement a policy and associated procedures for upgrading software, installing patches, and updating anti-virus signatures on all Department-owned mobile devices.
- Data contained on mobile devices shall be included in the Department backup policies and procedures.
- County policies regarding hard drive sanitization and equipment disposal shall be followed for all County-owned mobile devices.
- Use of a personally-owned (Employee owned) mobile device for County business purposes shall require approval from both the Department IT Manager and the Department/Agency Head, and shall require the Employee to sign a contractual agreement specifying the conditions for use, configuration, maintenance, and disposal of the device.
- Departments shall adhere to specified County procedures, as outlined in the *IT Security Incident Response Plan*, following loss or theft of a mobile computing device that is being used, or has been used, for County business purposes.

22.0 USB STORAGE MEDIA

This policy describes the requirements for the use, configuration, management, and disposal of USB storage devices, also called "thumb drives" and memory sticks.

- Each Department shall have a formal, written policy regarding the use of USB Storage Media, and shall disseminate this policy to its Users.
- Use of personally-owned USB Storage Media on any County-owned system is prohibited. All such Media used with County-owned systems shall be County-owned and formally issued to an individual User by that User's Department.

- Department-issued USB Storage Media are County property, and shall be used for legitimate County business purposes *only*. The same rules of conduct and appropriate use standards that apply to County-owned servers, desktop computers and mobile devices also apply to USB Storage Media.
- Use of USB Storage Media shall be limited to situations involving the simple transfer of data between computers, and not as a method for accomplishing a formal backup of data.
- Data contained on USB Storage Media devices shall be protected from alteration or disclosure via both authentication and privacy measures.
- Departments shall implement procedures for managing and controlling USB Storage Media.
- Departments shall implement methods to prevent the transfer of malicious software from USB Storage Media to County computers.
- Users issued USB Storage Media shall be responsible for the physical security of the device, and shall make every effort to protect USB Storage Devices from loss or theft.
- Following loss or theft of a County-owned USB Storage Media device, the procedures specified in the County's *IT Security Incident Response Plan* shall be followed.
- All USB Storage Media shall be treated as any other County-owned computing device for the purpose of device disposal.

ATTACHMENT A – GLOSSARY

Administrator: An individual whose job function or assignment is to configure, manage, and maintain County computer systems, including (but not limited to) servers, desktops, laptops, PDAs, and network devices. By definition, a designated "Administrator" will have higher access privileges than those assigned to a general User, including, but not limited to, the ability to: configure User accounts; install system software; change system configurations; run privileged system commands; reset passwords; review system and audit logs; and examine the files of other Users.

Agency/Department: Any reference to "Agency" or "Department" refers to both Agencies and/or Departments of the County.

Application Owner: A designated individual within a Department who is responsible for defining and enforcing the application's operating parameters, authorized functions, and security requirements.

Application Service Provider (ASP): An organization external to the County whose function is to "host" and support one or more applications used by a County organization.

Authentication: Process during which valid users are uniquely identified, and their identification is verified, prior to being given access to County information assets.

Authorization: Following authentication, the level of privileges that are assigned to individual users of IT resources.

Backup: The process of copying/duplicating files, databases, and/or system files to avoid loss of data and to facilitate recovery in the event of a system problem or failure.

Best Practices: Detailed, hands-on information for implementing and/or configuring the specified security procedures and standards. This information is provided as a separate document, the *IT Security Best Practices*, which is organized by operating system environment.

Business Application: Any software program that has been developed, acquired, or modified specifically to support a unique and identifiable County business function. This includes applications used by multiple Departments, such as CJIC and HaRP, and Department-specific applications such as AIMS (Assessor) and POPS (Pretrial Services).

Business Continuity Plan: A comprehensive statement of actions to be taken immediately following a disaster event to ensure the continuing operation of an organization's critical business functions.

Business Electronic Record: An electronic record that is created, received, stored, and/or maintained by a County employee in the transaction of County business, and that serves as documentation for and/or evidence of such activity.

Business Tool: A software program that is designed to support general office functions. This type of software includes word processing software, electronic mail software, utility software, or other general-purpose software such as Microsoft Word and Excel, Adobe Acrobat, Lotus Notes, etc. Note that if a "business tool" has been used as the basis for developing a unique software program to support a business function within a Department (for example, if Lotus Notes has been used to develop a Department-wide database system), then the resulting software falls into the category of a "business application."

Change Control: A combination of technical, physical, and procedural safeguards used to protect systems and/or software applications from unintentional and/or unauthorized modification.

Computer Incident Response Team (CIRT): County team of designated individuals responsible for planning and implementing a coordinated response to computer security incidents.

Confidential: This classification applies to information that is intended solely for use within the County and/or a specific County organization. Unauthorized disclosure of this data could adversely impact the County, its employees, and/or its business partners. Examples include internal telephone directories, organization financial data, and sensitive purchasing information.

Configuration Management: Procedures that support the capability to identify the exact configuration of a system and/or software application at discrete points in time for the purpose of systematically controlling and managing changes to the configuration.

County: For the purpose of this document, any reference to "County" is to be interpreted as "Santa Clara County."

County (Internal) Email System: An email system that has been established for the sole use of County employees, and is maintained, controlled, and managed by County IT staff. Internal County email systems provide messaging services using end user email addresses linked to the County domain name structure.

County Organization: The term of County organization is used semantically as County Agency/Department throughout the document.

Data/Information: Any business-related communication or information, whether numeric, graphic, or narrative, maintained on any medium, including computerized databases, paper, microform, optical/magnetic disk, magnetic tape,

and/or that is in transit over a communications network. No distinction is made between the word "data" and "information" for purposes of this policy.

Data Owner: An individual or business unit within a County organization designated as being responsible for classifying and controlling data owned, used, or generated by the organization.

Data Port: Wall-mounted outlet with plug-in jacks intended for use in connecting a computing device to a local area network. The typical data port supports local Ethernet LAN access.

Department Security Liaison: The person responsible for coordinating Department security awareness, and for acting as that Department's contact regarding IT security issues.

Disaster: Any event that affects an organization's ability to continue normal operations. "Disasters" can be due to any cause, including events of nature (such as floods, earthquakes, etc.), accidental circumstances (such as fire, burst pipes, failure of a critical server, etc.), or man-made (such as intentional denial of service attacks).

Disaster Recovery Planning: The advance planning and preparation necessary to minimize loss and ensure continuity of an organization's critical systems and IT infrastructure in the event of a disaster. The goal of Disaster Recovery is to restore functional operation of the critical systems and IT infrastructure as soon as possible.

Discussion Group: An Internet service that allows users to "post" messages, opinions, or other information to a general "bulletin board," where the messages can then be viewed by other members of the group. Typically postings to a discussion group or bulletin board are archived for some period of time and can be retrieved at a later date.

Electronic Protected Health Information (ePHI): Protected Health Information (PHI), as defined by the HIPAA rules and regulations, that resides on electronic media (to include computer memory devices, as well as any removable media such as magnetic tape or disk), or that is transmitted between electronic media via transmission media such as the Internet, leased lines, dial-up lines, or private networks. HIPAA security rules apply solely to ePHI. (See also Protected Health Information).

Electronic Record: information in a form that can be accessed only by a computer; a record that has been created and/or stored by electronic means, such as computer files, scanned images, or files on tape, disks, or in internal computer memory. The term Electronic Record is used within this policy to refer to both general electronic records as well as to the more specific email message.

Encryption: The process of scrambling information so that only someone that knows the appropriate key can obtain the original information.

HIPAA: Health Insurance Portability and Accountability Act. A Federal rule passed by Congress in 1996 designed to set national, minimum standards for the administrative, technical, physical and organizational protection of Protected Health Information (PHI).

Information Systems: Any combination of computer hardware and software that generates, processes, transmits, accepts, and/or stores data or information.

Informational Electronic Record: an electronic record that has been created to expedite County administrative business processes, but that does not contain official, business-related information subject to specific retention requirements. These types of records have short term facilitative value to the individual or work group, but their sole purpose is to provide information required to ensure the completion of a routine action or the preparation of a subsequent "official" record. These types of records include such things as meeting notices, reminders, informal notes, drafts of correspondence, and information downloaded from external web sites.

Infrastructure System: A computer system or device that is designed to support, or to provide services to, multiple Users and/or organizations; this includes servers, routers, switches, firewalls, and other network appliances.

Instant Messaging (IM): A popular type of application offered by many Internet service providers that allows "real-time" communication and file transfers between two or more individuals using the browser interface. The distinguishing feature of IM is that the architecture employs a centralized server managed by the Internet service provider, and this server controls communication between the participants.

Internet (External) Email System: Any email system or service that is external to the County, and that is provided and supported by an Internet Service Provider or other Internet-based entity for use by the general public, such as *hotmail*. Internet email systems are not maintained, controlled or managed by County IT staff, and utilize email addressing that is not related to the County's domain name structure.

IT Security Policies: A set of high level rules and requirements that represent the baseline for managing and protecting the County's IT resources.

IT Security Principles: The primary, baseline doctrines that serve as the basis of the County's IT Security Program. These IT security principles are contained in the Board of Supervisor's Resolution dated June 25, 2002, and are provided as Attachment A of this document.

Malicious Software: Software that has been designed with the specific intent to damage a computer or network, impede performance, disrupt operation, or destroy or alter data. Types of malicious software include, but are not limited to, viruses, worms, Trojan Horses, adware/spyware, and software intended to result in denial of service (DoS).

Metadata: is information that is used to describe data. For example, the header information in an email message is the metadata that describes that message and provides its context.

Mobile Computer: Any computing device that can be disconnected from one network and re-attached to another network. This includes portable devices such as laptop computers, Personal Digital Assistants (PDAs), smart phones, and Pocket PCs. This definition also includes desktop PCs in those circumstances where the desktop device is disconnected from one network and then re-connected to another network. Since wireless access devices work in this manner, they are also considered to be "mobile" computers for the purposes of this policy.

Mobile Device: Any portable computing device that is capable of receiving, storing, and/or processing data, including laptops, Pocket PCs, tablets, PDAs, "smart" phones (including iPhones), MP3 players (such as iPods), and USB memory sticks ("thumb drives"). In general, these devices typically run a bona fide operating system and have processing power sufficient to support one or more applications. However, USB thumb drives ("memory sticks") used solely for storing and/or transporting data are also included within the category of Mobile Device since in most cases they can be loaded with operating system software and applications. Simple pagers, cell phones capable *only* of making and receiving telephone calls, CDs, and floppy disks are not currently included in the definition of Mobile Devices.

Non-County Infrastructure: Any network or environment in which the device(s) and/or network equipment are not under the direct control and management of designated County IT network support staff. This includes, but is not limited to, vendor facilities, other Government facilities, employee homes, the Internet, and devices and/or networks in County facilities that are not directly connected to the County's CLARAnet network.

Non-Secure Communication: Any method of communication that could potentially allow disclosure of personal, private, restricted, or confidential data. This can include un-encrypted electronic communication, fax, hard-copy, or even verbal communication, depending on the circumstances.

Peer-to-Peer Connection (P2P): Also known as *file sharing*, P2P connections are a popular Internet application used for sharing and transferring messages and

files. The distinction between IM and P2P services is that P2P does not employ a centralized server, and participants are directly connected to one another (thus "peer-to-peer"). Each "peer" in the relationship may have one or more simultaneous connections to other devices.

Personal Digital Assistant (PDA): Small, portable, hand-held device that provides computing capability, as well as information storage and retrieval.

Personal Electronic Record: an electronic record that has been created and/or received by a User for casual, personal use, and that is not associated with valid County business processes, such as a personal email message.

Portable Computer: Any computing device that is small in size, and that is intended to be carried "by hand" from location to location. This includes laptops, PDAs, and "smart" cell phones capable of receiving, storing, and/or processing data.

Procedures: Specific steps, tasks, and activities to be performed to implement the approved *IT Security Policies*.

Protected Health Information: As defined by the HIPAA (Health Insurance Portability and Accountability Act), Protected Health Information (PHI) is "individually identifiable health information;" i.e., health information that can be associated with a specific individual. (See also Electronic Protected Health Information, ePHI).

Recordkeeping System: an electronic "system" designed to create, capture, store, protect, and/or control records or other data as evidence of business transactions, and that supports retrieval of these records or data. Any electronic information "system" that incorporates these functions can qualify as a recordkeeping system, including document management systems, business applications, simple on-line databases of business information, and organized folders of Excel spreadsheets and Microsoft Word documents.

Remote Access: Any access of County IT assets from a non-County infrastructure (including employee homes), no matter what technology is used to accomplish such access.

Remote Control Technology: Remote access technology that employs an architecture in which the remote device takes control of an internal, network-connected device, and through this mechanism becomes a "peer" on the internal network.

Restricted: This classification applies to information that is protected by statute, law, or regulation, or that has been identified as particularly sensitive and/or personal. This includes social security numbers and other personal identifiers, protected health information, and criminal justice information.

Retention Schedule: The length of time that an Electronic Record should be maintained before it is scheduled to be destroyed or archived. Once the record is destroyed, it is no longer retrievable.

Security Incident: Security incidents include, but are not limited to, the following: computer viruses or worms; Trojan Horses; Denial of Service; unauthorized and/or improper use of computer accounts or IT resources.

Standards: Configuration, implementation, or other guidelines established by general consent and approval as the criteria for determining compliance with the approved *IT Security Policies*.

Third-Party Remote Access: Remote access to internal County networks and IT resources by individuals other than County employees. This includes, but is not limited to, contractors, consultants, vendors, and employees of other Government organizations.

Two-Factor Authentication: A strong method of authenticating a user to verify that that user is in fact the individual he is claiming to be. The two-factor authentication approach requires that the user provide two of the following three items: something that the user has (such as a token card access device), something that the user knows (such as a password), and something that the user "is" (such as a fingerprint or retina scan). County approved two-factor authentication methods are described in the *IT Security Procedures and Standards* document.

Untrusted Network: Any data transmission network that is not under the direct management and control of County network support staff. Typically any network connection within the CLARAnet environment is viewed as "trusted," while the Internet is "untrusted."

USB Storage Media: any portable media device that is USB-based and is designed to store and/or transport electronic information between computer systems. USB Storage Media includes generic USB flash drives, also known as thumb drives, and memory sticks.

Users: Any reference to "Users" should be interpreted as individuals accessing and/or using County IT assets, including employees, contractors, consultants, part-time employees, volunteers, and any other authorized individuals attempting access or use of the County's IT infrastructure.

SECTION ___. BUSINESS ASSOCIATE AGREEMENT PURSUANT TO THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

I. Definitions

Terms used, but not otherwise defined, and terms with initial capital letters in this provision of the Agreement have the same meaning as defined under the Health Insurance Portability and Accountability Act of 1996, 42 USC §§ 1320d et seq. ("HIPAA") and the implementing regulations. To the extent the HIPAA Privacy Rule changes the meaning of the terms; this provision shall be modified automatically to correspond to the meaning given in the rule.

"PROTECTED HEALTH INFORMATION," as defined at 45 C.F.R. §§ 164.501, and 160.103, means information that:

(1) is created or received by a health care provider, health plan, employer or health care clearing house; and

(2) relates to the past, present of future physical or mental health or condition of an individual; the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual, and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)" as defined at 45 C.F.R. § 160.103(2), means Protected Health Information that is created electronically, transmitted electronically by electronic media, or is maintained in electronic media.

"BUSINESS ASSOCIATE" refers to _____ (Name of Contractor) in this Agreement.

"COVERED ENTITY" refers to the County of Santa Clara in this Agreement.

II. Duties & Responsibilities of BUSINESS ASSOCIATE

A. BUSINESS ASSOCIATE'S use and/or disclosure of PROTECTED HEALTH INFORMATION ("PHI") will be limited to those permitted or required by the terms of this Agreement or as REQUIRED BY LAW as defined pursuant to 45 CFR 164.501.

B. Unless otherwise limited by this Agreement, BUSINESS ASSOCIATE may use the PHI in its possession for the proper management and administration of the BUSINESS ASSOCIATE or to carry out its legal responsibilities.

C. BUSINESS ASSOCIATE may further disclose PHI for the proper management and administration of the BUSINESS ASSOCIATE or to carry out its legal responsibilities if the disclosure is required by law, or the BUSINESS ASSOCIATE receives reasonable assurances from the person receiving the PHI that it will be held confidentially, and will be used or further disclosed only as required by law and that the person receiving the PHI will notify the BUSINESS ASSOCIATE of any instances known in which the confidentiality has been breached.

D. BUSINESS ASSOCIATE must not use or disclose PHI in any manner that would constitute a violation of the PRIVACY RULE (Standard for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subpart A and E).

E. BUSINESS ASSOCIATE must use appropriate safeguards to prevent uses or disclosures of PHI other than as provided for by this Agreement.

F. BUSINESS ASSOCIATE must report in writing any use or disclosure of PHI not provided for by this Agreement to the COVERED ENTITY as soon as it learns of it.

G. BUSINESS ASSOCIATE must ensure subcontractors and agents that have access to, or to whom the BUSINESS ASSOCIATE provides PHI, agree in writing to the restrictions and conditions concerning the use and disclosure of PHI which are contained in this Agreement.

H. At the request of the COVERED ENTITY, BUSINESS ASSOCIATE must comply with the COVERED ENTITY'S request to accommodate an individual's access to his/her PHI in a designated record set maintained by the BUSINESS ASSOCIATE. In the event an individual contacts BUSINESS ASSOCIATE directly about access to PHI, BUSINESS ASSOCIATE will not provide access to the individual but will forward the request to the COVERED ENTITY within three business days of contact.

I. Within fifteen business days of a request by the COVERED ENTITY, BUSINESS ASSOCIATE will comply with the COVERED ENTITY'S request to amend an individual's PHI in a designated record set maintained by the BUSINESS ASSOCIATE. BUSINESS ASSOCIATE will promptly incorporate any such amendment into the PHI. In the event an individual contacts BUSINESS ASSOCIATE directly about making amendments to PHI, BUSINESS ASSOCIATE will not make any amendments to the individual's PHI but will forward the request to COVERED ENTITY within three business days of such contact.

J. BUSINESS ASSOCIATE must keep a record of disclosures of PHI for a minimum of six years and agrees to make information regarding disclosures of PHI available to the COVERED ENTITY within fifteen days of a request by the COVERED ENTITY. BUSINESS ASSOCIATE must provide, at a minimum, the following information:

(1) the name of the individual whose PHI was disclosed.
(2) the date of disclosure;
(3) the name of the entity or person who received the PHI, and the address of such entity or person, if known;
(4) a brief description of the PHI disclosed; and
(5) a brief statement regarding the purpose and explanation of the basis of such disclosure.

BUSINESS ASSOCIATE is not required to maintain a record of disclosures of PHI under the following circumstances:

(1) To carry out treatment, payment or County health care operations, or activities that are incident to such disclosures;
(2) To individuals of their own PHI;
(3) Pursuant to a written authorization;
(4) For the facility's directory or to person involved in the individual's care or other notification purposes in 45 CFR 164.510;
(5) For national security or intelligence purposes;
(6) To correctional institutions or law enforcement officials;
(7) As part of a limited data set in accordance with 45 CFR 164.514(e); or
(8) That occurred prior to the compliance date for the covered entity.

K. BUSINESS ASSOCIATE must comply with any other restrictions on the use or disclosure of PHI that the COVERED ENTITY may from time to time request.

L. BUSINESS ASSOCIATE must make its internal practices, books and records relating to uses and disclosures of PHI available to the Secretary of the U.S. Department of Health and Human Services or designee, for purposes of determining the COVERED ENTITY'S compliance with the PRIVACY RULE. BUSINESS ASSOCIATE must notify the COVERED ENTITY regarding any information that BUSINESS ASSOCIATE provides to the Secretary concerning the PHI. Concurrently with providing the information to the Secretary and upon the COVERED ENTITY'S request, BUSINESS ASSOCIATE must provide COVERED ENTITY with a duplicate copy of the information.

M. Upon the termination of this Agreement for any reason, BUSINESS ASSOCIATE must return or destroy all PHI, including all PHI that is in the possession of subcontractors or agents of the BUSINESS ASSOCIATE. BUSINESS ASSOCIATE must not retain any copies of PHI. If return or destruction is not feasible, BUSINESS ASSOCIATE must notify the COVERED ENTITY of the condition that makes the return or destruction of PHI not feasible. If the

COVERED ENTITY agrees that the return or destruction is PHI is not feasible, BUSINESS ASSOCIATE may dispose of the PHI, subject to all of the protections of this Agreement and must make no further use or disclosure of the PHI.

N. The respective rights and responsibilities of BUSINESS ASSOCIATE related to the handling of PHI survive termination of this Agreement.

O. Notwithstanding any other provision of this Agreement, the COVERED ENTITY may immediately terminate this Agreement if BUSINESS ASSOCIATE has materially violated its responsibilities regarding PHI under this Agreement upon written notice.

P. **EPHI**: If BUSINESS ASSOCIATE receives, creates, transmits, or maintains EPH on behalf of COVERED ENTITY, BUSINESS ASSOCIATE will, in addition, do the following:
   (1) Develop, implement, maintain and use appropriate administrative, physical, and technical safeguards in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320(d) or the United States Code and Title 45, Part 162 and 164 of CFR to preserve the integrity and confidentiality of all electronically maintained or transmitted PHI received from or on behalf of COVERED ENTITY.
   (2) Document and keep these security measures current and available for inspection by COVERED ENTITY.
   (3) Ensure that any agent, including a subcontractor, to whom the BUSINESS ASSOCIATE provides EPHI agrees to implement reasonable and appropriate safeguards to protect it.
   (4) Report to the COVERED ENTITY any Security Incident of which it becomes aware. For the purposes of this Agreement, Security Incident means, as set forth in 45 C.F. R. section 164.304, “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”

Training Methodology

Best Practice Guideline Sources

International Society for Performance Improvement Guidelines (ISPI)
Instructional Design Standards. (usability, technology standards, accessibility)
Kilpatrick Levels of evaluating of learner performance
Adult Learning Theory
Consider Unique Clinic Structure and Clinic Culture

Training Plan

The Training Team has developed a training plan to address all areas of training for all level of users. Training will include a mix of: Kick Off Meetings, Instructor Lead Training, Just In Time Training and Self Guided On Line Learning. Materials will include: Videos, web based instruction, pocket manuals, end user and trainer manuals and brown bag lunches.

Trainer Credentialing

This one (1) week program will credential each participant in the training methodology and provide for a standardized approach to training. Each participant will finish the program and be ready to train. Trainers and super users will go through the credentialing program.

End user proficiency assessments

Competency ensures readiness for use and will be measured by a combination of on line evaluation and end user demonstration.

Training Kick Off Meetings

A series of four (4) meetings will occur during the rollout of the project. These meetings are designed to provide training information ahead of training time. The goal of each meeting is to address important information regarding training at each stage.

- Initial Kick Off Meeting – Two (2) months prior to first Training (Will be held in a central location for any end user to attend)
- Site Kick Off Meeting – One (1) month prior to clinic Training
- Site Readiness – Two (2) weeks prior to live

Classroom Instructor Lead Training

Role and Workflow based (day in the life) scenarios will be used and include videos of “messages from the Sponsors”, demonstrations, “dress rehearsals”, and other training methods.

Self Guided On Line Learning

Reusable, Re-Deployable, available electronically, will accommodate bringing up new users and as refreshers. Will include end user proficiency testing, can be started and stopped based upon end user availability. Most importantly it should be easy to access, intuitive, and interactive.

Training Effectiveness Evaluations, Training Tracking and Training Completion Reporting

Trainers will report weekly regarding # of users trained and % passing competencies. Training will report on top issues from end user evaluations of training and remediation plans weekly.

Training Methodologies

Appendix B-11

Types of Training Materials	
Videos/DVDs	Video recordings of Stages in action at clinics.
Power Point (w/plug in)	Can be used as an eLearning tool with interaction or presentations.
Visio	Can be used to demonstrate clinic workflow, etc.
eLearning Software	Software that provides for user interaction and learning.
Testing Software	Software that provides the ability to test end users and score competency.
Manuals	Using Microsoft Word or similar; create end users manuals for reference.
Quick Guides	Short guides that help end users reference commonly used features.
Cheat Sheets	One page sheets that explain to end users how to complete a task or tasks.
Pocket manuals	Small, short manuals that provide a quick reference to commonly used features.
Flip Cards	Similar to a pocket manual but can be used to provide quick references to commonly used features.
Flyers	Used to communicate a new feature, change, etc.
Newsletters	Used to communicate a new feature, change, etc.
OnLine Help (? in EMR)	Electronic help
Help in EMR	Electronic help
Email communication/reminders	Electronic communication method
Posters	Used to communicate a new feature, change, etc.
Provider training guide attached in EMR	Electronic reference help

Methods for delivering training	
Classroom Instruction	Teaching method in which students learn in a classroom environment with instruction, demonstration and practice. Formal scheduling is usually required.
Ad Hoc Training	Training method in which students learn when needed or requested. No formal scheduling required.
Just in Time training	Training method in which students learn when needed or requested. Scheduling can be formal or provided “just in time”.
eLearning	Training method in which students learn in an electronic environment with interactive software. Formal schedule is set to complete the eLearning but not when students actually take the eLearning course.
Elbow to Elbow training	Training method in which students learn in an informal environment with an instructor. No formal scheduling required.
Super user training	Training method in which student learn from peers in either a classroom or elbow to elbow training style. Formal scheduling may or may not occur.
Dress Rehearsal training	Training method in which students learn from demonstrating what has been taught. This learning style provides students the ability to increase comprehension and retention.
Demonstrations (by training team, etc.)	Training method in which students learn from watching a demonstration of the material in action. Demonstrations can be delivered by videos or other methods.
Videos	Training method in which material is presented in action via a video.
CD/Thumb Drives	Training method in which training can be completed outside of a classroom.
Brown Bag lunches	Training method in which training can be delivered over shorter amounts of time with a focused audience. Formal scheduling may or may not occur.

Section 1 – SCVHHS Information Services Overview

Mental Health Systems / Alcohol and Drug Service Systems

Mission Statement

To provide the highest quality IS applications, data analyses and user support to the Mental Health and the Department of Alcohol and Drug Services. This support will offer the technology needed to assist both departments in improving the health and quality of life of their clients, and to support the mission of SCVHHS.

The MH / DADS IS purpose and responsibilities are:

- **Applications**
  - Unicare, the MH and DADS billing application. Operations provides application support by offering a team of analysts dedicated to Unicare. Includes server maintenance, application maintenance, ODBC configuration, database tuning, installation of new patches and releases when available. Responsible for all user accounts and support of their workstations, including circuits, terminal servers, and training. Work collaboratively with HHS IS Technical support.
  - AVATAR Methadone Dispensing System: M4 application upgraded to AVATAR. Maintain application, user training and troubleshooting. Download AVATAR service data into Unicare. Upgrades when necessary.
  - Computrust Financial System: Responsible for support of the MH Representative Payee Computrust application. Includes server configuration and support, application upgrades, and monthly data file transfer.

- **Other Operations**
  - Responsible for building and processing of reports, system configuration for claims processing, CSI CalOMS reporting to the state. Also responsible for state Performance Outcome Measure Database access for the Mental Health Services Act (MHSA) client outcomes data entry.

- **System Access (in collaboration with HHS IS Technical Services)**
  - Provides remote access and/or Thin Client access into the Unicare system. Coordinates with Technical Services for completion of network design and closet builds for all non-county MH and DADS sites.

- **Mental Health DIAMOND**
  - Responsible for the DIAMOND application system, including the configuration, maintenance and operation of the system which includes fixing user errors and issues, phone support for application and technical questions, staff training and user manual production, FTP and TAR of data files, EDI and data transfer, archiving, submission of Medi-Cal and MH CSI encounter data to the State, participation in MH strategic planning to support the Managed Care business functions and to meet government regulations.

Appendix C: Technology Needs Assessment

Guide to Appendix C Documents

Appendix C-1:	Overview
Appendix C-2:	MHSA IT Planning Project Schematic
Appendix C-3:	MHSA IT Planning Project Overview
Appendix C-4:	MHSA Technological Needs Project Organization
Appendix C-5:	MHSA IT Roadmap
Appendix C-6:	Training Schedule

Technology Needs Overview

Santa Clara County issued an RFP to obtain consulting services to assist in the preparation of their MHSA IT Request. Outlook Associates, LLC. was selected to provide support and assistance to the project. A summary of the project can be found in Appendix C-2 and Appendix C-3.

During the course of the project, over fifty individual and group interviews were conducted with stakeholders from the Mental Health Department, Provider organizations, IS Department, other County agencies, Contract Provider agencies and consumers to solicit their opinion of the current IT environment and obtain their ideas for technology functions that would assist them. From these meetings and interviews, seven IT projects were identified, presented and discussed with MHD Staff, IS Staff and community stakeholders. The seven projects were identified in the MHSA CFTN Enclosure 1 document which was approved by the State early in 2009.

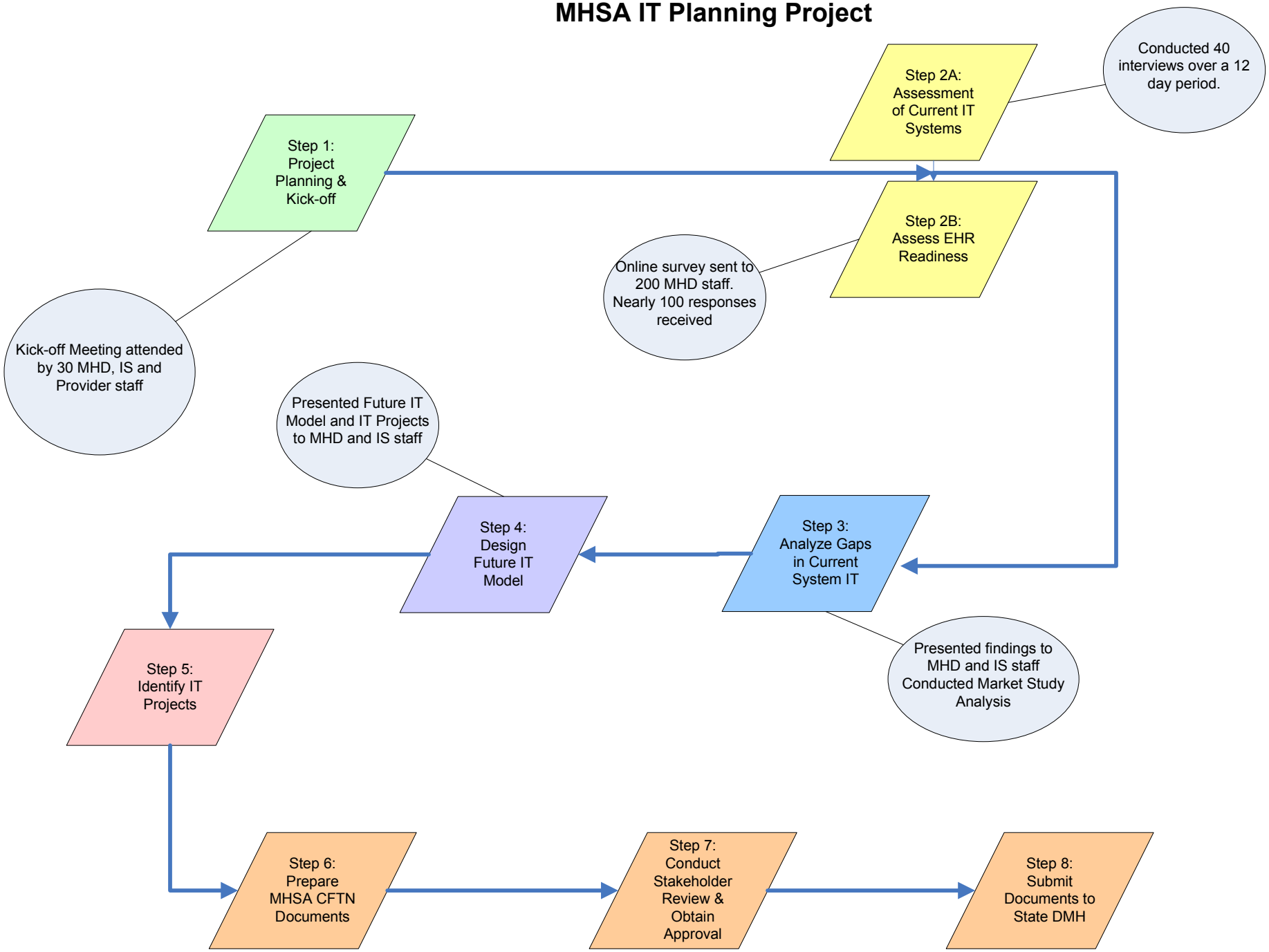
Once the projects were identified and approved by the stakeholders, MHD and IS recognized the need to create a new project organizational structure to coordinate resources and monitor all of the MHSA Technology projects. See Appendix C-4 to find an overview of the roles and responsibilities for these projects.

To view how the projects fit into the IISI infrastructure see the IT Roadmap in Appendix C-5.

Appendix C-6 contains a draft of the training schedule for the EHR project. The training plan will be fully developed during various stages of the EHR project. The plan cannot be completed until the vendor is selected and the implementation plan completed. SCVHHS MHD realizes that training is critical to the success of all of these projects. The SCVHHS established guidelines found in Appendix B will assist in the planning process.

Appendix C-2

SCVHHS MHD
MHSA IT Planning Project



MHSA IT Planning Project

	Activity	Results
Step 1:	**Project Planning & Kick-off Meeting** • Developed project plan and approach	• Held Kick-off Meeting 6/17/08 • 30+ MHD & IS Staff attended
Step 2:	**Assess Current State IT** • Obtain a picture of what systems support MH operations and how effective IT is within organization • Conducted EHR Readiness Survey to determine staff opinions on current IT challenges	• Conducted 40 individual and group interviews over 12 days • 58 MHD & IS Staff • 18 Contract Provider Representatives from 8 different Agencies • Visited 3 provider sites • 20 Consumers / family members • Met with 4 other County agencies • Conducted conference call with current IT vendor (Uni/Care)
Step 3:	**Analyze Gaps** • Determine what is missing to meet IISI standards and other Federal, State, and local IT mandates and needs of stakeholders	• Prepared Gap Analysis Report • Presented findings to MHD and IS Staff • Conducted Market Study Research for Behavioral Health EHR products
Step 4:	**Develop Future IT Model** • Prepare a high level overview of what IT will look like in 2014	• Presented IT Model to MHD and IS Staff
Step 5:	**Identify IT Projects** • Identify MHSA IT Projects	• Presented IT Project list to MHD and IS Staff • Facilitated discussion of projects • Finalized list of seven IT projects
Step 6:	**Prepare MHSA Documentation** • Draft Enclosure 1 & Enclosure 3 documents	• Drafted Technical Needs portion of Enclosure 1 document • Received approval of Enclosure 1 in early 2009 • Drafted Enclosure 3 documentation • Posted Enclosure 3 documents for public comment on 4/17/09
Step 7:	**Internal Review & Approval of Documentation**	• Met with MHD and IS staff to review project documentation • Posted Enclosure 3 documents for public comment on 4/17/09
Step 8:	**Submit Documents to State DMH**	

Project Organization

SCVHHS Executive Management Group (EMG)

- Provide Overall Project Guidance
- Provide insight to organization issues and requirements

Nancy Pena Ph.D., Bruce Copley, Deane Wiley Ph.D. Martha Paine, Dennis Kotecki, Michael Meade MD, Tiffany Ho MD, Janette Ferris, Pat Garcia
Project Sponsors

- Provide executive accountability for project success
- Set strategic plan
- Ensure organizational support for the project
- Demonstrate departmental ownership
- Provide guidance and support in resolving organizational issues or barriers. Ensure appropriate delegation of authority
- Make decisions in regards of scope, budget, timeline and resources. Make policy and process decisions
- Final approval of all deliverables

Cheri Silviera
Project Oversight

- Project Advisory
- Work with the Project Leadership Dyad to oversee the successful implementation of the project
- Review all project documentation and provide a wellness check to Project Sponsors.

Clinical Project Director (TBD)
Sue Clements
Project Leadership Dyad

- Direct overall project activities
- Provide oversight, management and guidance to each of the Project Implementation Partners
- Provides direction related to project approaches, schedules, resource and deployment
- Coordinate the organization across multiple functional areas
- Ensure communication to appropriate stakeholders
- Provide project management knowledge, tools and processes using a project management methodology and maintenance of an accurate project management plan.

Independant
Project Oversight

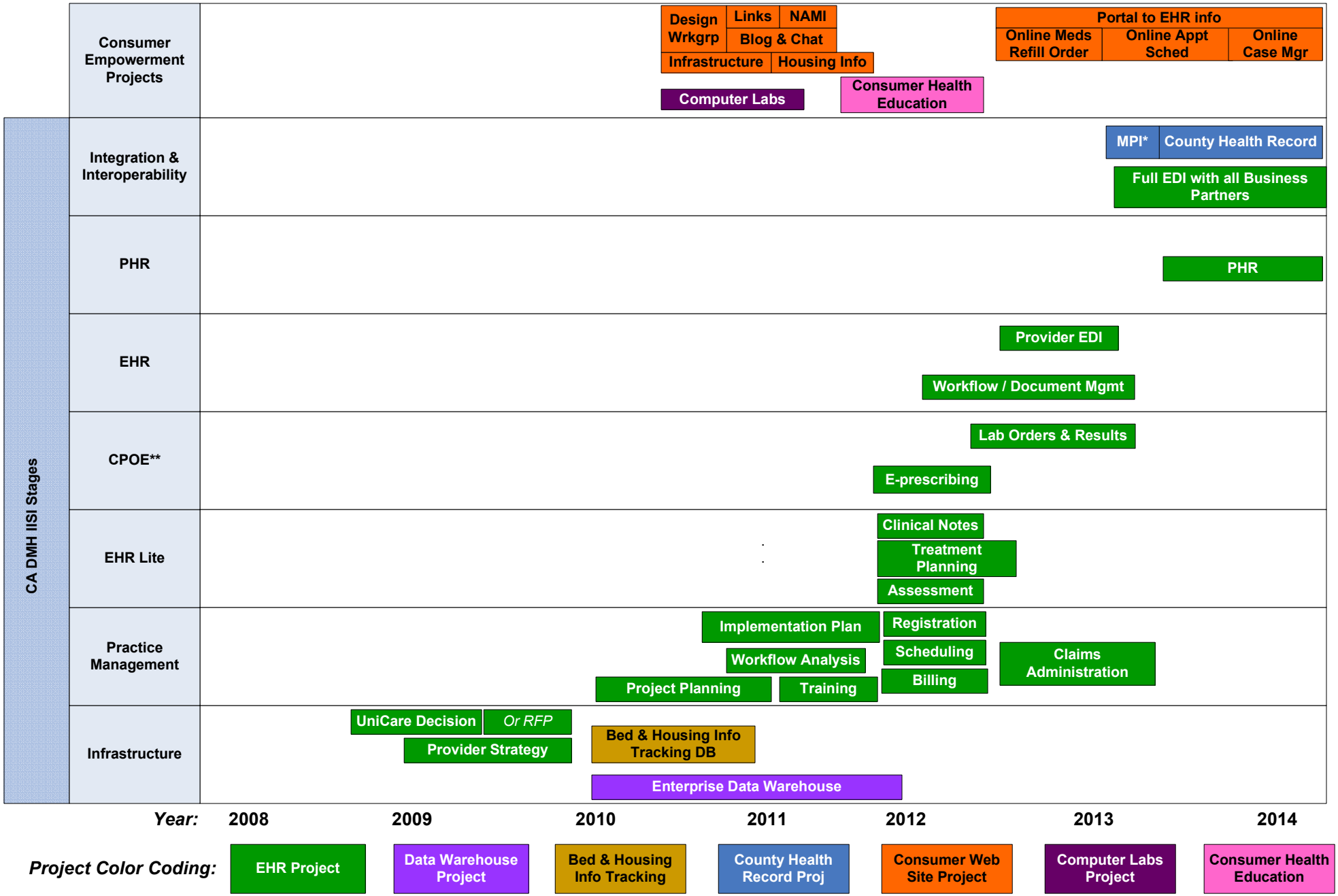
Clinical Business Coordinator (TBD)
Jeff McDaniel
Project Implementation Partners

- One Set of Implementation Partners for each of the 7 MHSA projects
- Work closely with clinical staff. Understand the clinical and business processes
- Champion clinical automation
- Execute, monitor and control the project by verifying project plans and managing day-to-day project activities
- Engage with stakeholders to remove barriers for the project teams

Electronic Health Record
Enterprise-Wide Data Warehouse
County Health Record
Bed and Housing Exchange Database
Computer Learning Center
Consumer Portal &Web Redesign
Consumer and Family Health Education

SCVHHS MHSA IT Planning Project

IT Roadmap



* MPI = Master Patient Index
** CPOE = Computerized Prescribing & Order Entry

4/15/2009

Appendix C-6

SCVHHS MHD EHR Project
Training Schedule

	2010												2011												
	Jan	Feb	Mar	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Ongoing
Project Management Overview & Planning	x	x	x																						
Project Technical Team Training											x	x	x	x											
Project Team Application / Analyst Staff Training											x	x	x	x											
Train the Trainer (Training Staff)													x	x	x										
Basic Computer Skills Training																x	x								
Super User Training																		x	x						
Technical Support Training																		x	x						
End-User Training																				x	x	x	x	x	x
Training Competency Evaluations																				x	x	x	x	x	x

Assumptions:

1. Training schedule assumes project initiating in January 2010
2. Project Management classes will be offered to managers to acquaint them with Information Technology project methodology so that they will be able to understand how to read and interpret the project tools. These classes will begin prior to project implementation.
3. Basic computer skills will be offered to staff that are not familiar with PCs. These people will be identified through a survey and interviews. These classes will begin prior to any system specific training.
4. Specific training will be determined during the project planning and design phases, after an EHR vendor has been selected.