Overview of M. D. Anderson’s Information Technology

The document that follows presents an overview of the information technology infrastructure at The University of Texas M. D. Anderson Cancer Center, including its data centers, networks, servers, desktops, applications, as well as information security and compliance requirements.

It is important to note that specific product versions, releases, patch levels, etc. are not detailed in this document as they can vary considerably with time. For example, while Microsoft Internet Explorer is adopted as a standard web browser product, only a specific set of versions may be supported for use at the Institution. Vendors responding to a Request for Proposal (RFP) are therefore asked to verify currently supported versions of products when appropriate.

**Data Centers**

M. D. Anderson operates two major data centers: (1) a 12,000 square foot primary data center located in the Main Campus and (2) an 11,000 square foot Co-Location Center located in Northwest Houston. This second facility is currently undergoing significant expansion in order to support our growing disaster recovery programs, along with those of nearby University of Texas System component institutions.

The majority of M. D. Anderson’s mission critical computer applications are housed at the primary Data Center, running on an IBM mainframe with an MVS/ESA operating system, DEC Vax minicomputers, Red Hat Linux, IBM AIX, and Microsoft Windows 2003. Key details about our data centers include:

- IBM Z890 mainframe (710 mips) with 38 terabytes of storage at the primary facility,
- IBM Z800 mainframe (up to 300 mips) with 19 terabytes of storage at the Co-Location Center facility,
- HP-C6000 1072 AMD processor-based high performance computing cluster with over 2 terabytes of distributed memory and infiniband interconnects, for research applications.
- HP 32 processor SMP Itanium system with 128GB of shared memory for research applications needing very large memory.
- 100 IBM P-Series open systems with 133.5 terabytes of storage,
- 45 terabytes of storage in HP-EVA systems for research based data. One VAX Cluster and 2 Alpha systems, and
• Total data storage (including both data center facilities) is currently approaching 400 terabytes.

**Networks**

M. D. Anderson operates a campus-wide Ethernet data communications backbone that connects all campus locations for purposes of electronic mail and other collaboration, access to web-based resources, and access to numerous application systems and databases. Key details about our networks include:

• Over 60,000 ports with 30,000 currently active nodes,
• Over 600 LAN switches, 1,200 wireless access points and 30 routers, and
• Connectivity provided to all Main Campus locations, South Campus locations, Science Park facilities in Bastrop County, Texas, as well as several outreach facilities across the Houston metropolitan area.

Network assets include: fiber and copper cable infrastructure, network switches and routers, SAN switches, wireless access points, terminal servers, uninterruptible power supplies (UPS), as well as network sniffers, probes and other monitoring tools.

**Servers**

M. D. Anderson has deployed over 800 servers operating under various operating systems. While Microsoft 2003 Server, IBM AIX and Red Hat Linux platforms are currently supported. It should be noted that although not necessarily our preferred server solutions), many applications are Novell Netware, Microsoft Windows NT and 2000, or Macintosh OS server based. The Institution has deployed a high performance computing cluster supporting genomics, population studies and other research activities, along with a high availability computing cluster that supports financial systems.

For the research community, the Institution has deployed a high performance computing cluster supporting computational Biology, Genomics, Population studies and other research activities, along with a high availability computing cluster that supports financial systems. The Institution has a 4-node HP Itanium based Oracle10g cluster attached to the EVA storage in the primary datacenter that is replicated in the co-location center with a similar HP-EVA storage system. An application development/production is deployed as well; clustered production systems, with separate development, test, staging systems, all based on Redhat Linux.

We have deployed a large storage array network (SAN) installation within our primary data center, managed using Tivoli Storage Manager. Several other large (Microsoft Windows) servers currently support our campus-wide e-mail, collaboration, and groupware needs.

M. D. Anderson has implemented numerous Hewlett Packard servers in clustered, active/active, active/passive or standalone (enterprise server) configurations. There are currently over 16,000 customers across the campus connected to this large set of enterprise servers. M. D. Anderson is
currently migrating our server infrastructure to one based on Microsoft Exchange 2007, an enterprise-wide Active Directory, and Microsoft based file and print services.

A small number of specialized departmental applications run on the Sun SPARC Station platform with Sun OS (Unix) as the operating system.

**Telecommunications**

M.D. Anderson operates a campus-wide Avaya telecommunications system and ATM (Asynchronous Transfer Mode) network backbone that connects all campus locations for purposes of telephone communications, voicemail, long distance, and access to associated adjuncts. Key details about our system and network include:

- Over 26,000 ports with 34 cabinets operating on a single switch platform supporting all of the owned and leased buildings throughout the Main and South Campus locations.

- The platform includes both traditional TDM (Time Division Multiplex) and VoIP (Voice over Internet Protocol) switching.

- The supported adjuncts include: Octel Voicemail (2 – 250’s & 1 - 350), ACD (Automatic Call Distribution) including a comprehensive statistical reporting module and Vocera.

- T1 Connectivity is provided to the Fax Server, Bed Management System, and other adjunct applications. Call recording is provided by an IP-connected Witness call recording system.

- Connectivity to the Science Park facilities in Bastrop and Smithville are provided over point-to-point T1 facilities to two independently operating Avaya telecommunications systems.

- Outreach facilities are connected to the campus-wide Avaya telecommunications system using VoIP technology. Over 200 VoIP telephones are deployed.

- Interactive Voice Repone (IVR) utilizes text-to-speech technology to initiate calls to patients and administer surveys for clinical departments.

- CTI (Computer Telephony Integration) is delivered via the Avaya Interaction Center to multiple departments.

- T1, DS3, OC3, GigaMAN, DecaMAN, OPT-E-MAN and ISDN-PRI provide the wide area connectivity.

- BES (BlackBerry Enterprise Server) platform supports over 3,000 BlackBerry devices with pager integration.

Telecommunications assets include: fiber and copper cable infrastructure, as well as uninterruptible power supplies (UPS).
**,Desktop Systems**

M. D. Anderson currently supports over 23,500 desktop (and notebook) computers. Microsoft Windows XP has become the predominant desktop operating system, with approximately 2,500 Macintosh systems OS based personal computers being used in select areas of the campus.

M. D. Anderson has adopted several desktop computing related standards, including Lotus Notes for collaboration (electronic mail, calendaring, and collaboration), Microsoft Office (word processing, spreadsheets, presentation graphics, and databases), as well as the Internet Explorer, Safari, and Firefox web browsers. Other established standards include: Trend Micro OfficeScan, Adobe Acrobat Reader, the Novell Netware client and ZENworks, and the Altiris Client Management Suite. (Both of the Novell products will eventually be removed from our standards as Microsoft file and print services as well as Altiris Client Management are implemented across the enterprise; furthermore, M. D. Anderson is currently migrating from Lotus Notes to Microsoft Exchange based messaging.)

From a hardware perspective, M. D. Anderson currently acquires Windows based systems from Dell along with Apple systems based on the Macintosh operating systems, as well as HP desktop printers and scanners. Finally, M. D. Anderson utilizes the Citrix environment for cross-platform access via institutional standard desktop computers.

Finally, M. D. Anderson has prepared a list of institutionally approved and supported desktop computing products, along with other preferred software titles. The most recently published *M. D. Anderson Information Technology Standards* document is provided as a detailed attachment.

,**Applications**

There are approximately 175 major applications in use at M. D. Anderson in support of our clinical care and education missions as well as institutional operations. In addition, over 10,000 databases of various scope and size have been developed and implemented.

Over 150 applications for the research community in the fields of Genomics, Proteomics, Drug development/ drug discovery, Molecular modeling and Bioinformatics along with numerous molecular biology databases are implemented.

,**Commercially Available Applications**

Major commercially available application systems for administrative, financial, and some clinical areas that are in use at M. D. Anderson include:

- **Administrative/Financial Applications**
  - HCC (cost accounting, contract management)
  - Hyperion Planning (budgeting and forecasting)

- **Hyperion Enterprise** (financial consolidation)
- **Hyperion Strategic Finance** (economic modeling)
- **Hyperion BI+** (reporting and analytics)
• SmartStream (State of Texas Regents budgeting)
• IDX (physician billing)
• Kronos (automated time and attendance)
• Lawson (asset management, inventory control, general ledger, accounts payable, supply chain)
• Infor (GEAC general ledger)
• PeopleSoft (payroll, human resources management)
• Mainsaver (computerized maintenance management)
• Siemens Building Management
• Siemens Invision (hospital and clinic billing)

**Patient Care Applications**

• Apollo (cardiology)
• Centricity (pharmacy)
• Cerner (blood bank and laboratory) – to be replaced near-term with MAK blood bank and SOFT laboratory applications
• Eclipsys (chart management)
• IMPAC (radiation oncology)
• Impath (anatomic pathology)
• LanVision (scanned patient records)
• MAK (blood bank)
• MaxSys II (care management)
• McKesson APS robot pharmacy system
• Mediserve (respiratory care)
• PICIS (anesthesiology and critical care)
• Pyxis (medication distribution)
• Siemens Invision (ADT, census, patient management)
• Siemens Novius (radiology)
• Stentor (PACS)

**Internally Developed Applications**

In addition to the above set of key commercially available applications, a considerable amount of internal software development occurring at M. D. Anderson, notably including ClinicStation (the institutional electronic medical record), ResearchStation (for research nurses), and the TissueStation tissue banking system.

ClinicStation provides a single source of clinical information needed to support our clinical care and research operations. Developed using a services oriented architecture (SOA) framework, ClinicStation provides online gateways to information maintained in other systems, including those supporting diagnostic imaging, laboratory, pathology, pharmacy, etc., in a highly integrated manner. M. D. Anderson is currently developing, deploying and enhancing the ResearchStation and TissueStation applications for our world-class research community. These applications are being built around the principles of integration with our suite of clinical systems as well as collaboration with external cancer research efforts.

All applications supporting M. D. Anderson’s Basic and Translation Research areas are either web services enabled, or web based in their current state. They are integrated into other systems where ever appropriate. They are primarily in the J2EE environment and/or a combination of Perl/PHP/Java technologies.
Other internally developed applications in used at M. D. Anderson currently include:

- CORe (Clinical Oncology Research System)
- FReD (management of grants, contracts and other sponsored agreements)
- Involved Provider Database
- myMDAnderson.org (customized patient and physician portal)
- PDMS (Protocol Data Management System)
- RIMS (Research Information Management System)
- Single point information data repository (SPiDR)

**Application System Standards and Directions**

M. D. Anderson has adopted the following information technology related frameworks, standards and strategic directions:

- CSSP (web page layout control)
- HL7 clinical data protocol
- J2EE environment (e.g., Tomcat, JRun)
- LDAP based authentication
- Operational Data Stores (ODS)
- Services Oriented Architecture (SOA) framework
- VMWare for server virtualization
- XHTML 1.0 based web pages
- Business Objects XI Enterprise (Crystal Reports XI)
- Hyperion Financial Reporting
- Hyperion Interactive Reporting
- Hyperion Web Analysis
- Microsoft Active Directory
- Microsoft Exchange Server and Microsoft Outlook
- Microsoft .NET Framework (with Avanade ACA.NET extensions)
- Microsoft SharePoint
- Microsoft SQL Server or Oracle platforms for databases
- Microsoft Team Foundation Server
- Microsoft Visual Studio
- Microstrategy Report Services
- Microstrategy OLAP ServicesOracle DBMS
- Percussion Rhythmix (web content management)
- Quovadx Cloverleaf integration engine
- Documentum (enterprise document management)
- ImageNow (administrative document management)
- Stentor (medical imaging)
Information Security and Compliance Requirements

M. D. Anderson has a comprehensive information security program that includes an ongoing risk assessment, disaster recovery planning, as well as incident prevention and management. Supporting incident prevention and management efforts are a variety of security tools, including desktop and server anti-virus, intrusion detection and prevention systems, multiple firewalls, etc. Additionally, an identity management program, currently based on Shibboleth and Novell eDirectory, is in place across the enterprise. Finally, M. D. Anderson is currently implementing Microsoft Active Directory with central LDAP-based authentication as part of a large infrastructure upgrade project.

M. D. Anderson has established the following information security guidelines based on regulatory requirements and security best practices:

Administrative Safeguards

- Proper auditing should be in place and comply with M. D. Anderson Policy. Auditing logs should be retained and reviewed regularly according to M. D. Anderson Policy. Logs for systems containing electronic protected health information must be kept for a period of 6 years.

- Applications should provide a means to allow granular access to the system in order to facilitate the user’s ability to perform only the actions necessary to carry out their job duties.

- Account administration functions should be informed of terminated employees in a timely fashion. User accounts creation, modification and deactivation is to be managed (centrally) by the Accounts Services Team in the Information Security Department.

- Access to M. D. Anderson’s information resources requires assignment of unique User IDs and passwords for each system user. Granting of vendor accounts must follow M. D. Anderson’s Security Network Connections Agreement.

- All systems, including those approved by the Food and Drug Administration (FDA) must have a method defined by which they can be patched/updated in a timely manner in order to respond to new security vulnerabilities. At a minimum, a system should support the use of current institutional standards such as the Trend Micro client and the Altiris agent.

- Applications should “lock” accounts after no more than 5 incorrect logon attempts have taken place, in accordance with M. D. Anderson Policy.

- Applications should ensure adherence to established M. D. Anderson password policies and naming conventions.

- Critical applications should provide for alternate modes of operations and/or disaster recovery capabilities when necessary.
• Vendors will be required to provide a service level agreement to include the assurance of reasonable time frame for addressing security related issues.

Physical Safeguards
• All servers related to the application should be able to be housed in a secure facility such as the M. D. Anderson data center.

• Final disposition of electronic confidential and restricted confidential information, and/or the hardware or electronic media on which it is stored must occur in a manner compliant with institutional policy and relevant security and privacy regulations.

Technical Safeguards
• Applications should support “strong” authentication and not pass user IDs and passwords across the network in “clear text.” Although encryption of transmission within the M. D. Anderson network is not a requirement, it is strongly recommended.

• Applications should facilitate a process for emergency access during either planned or unplanned outages. If the system administrator is not available, then there should be procedures for obtaining necessary electronic protected health information during an emergency.

• Applications should provide a method to automatically “log off” users after 15 minutes of idle time.

• Applications should accommodate measures to effectively address where data is stored but also how it is transmitted between locations, including the use of encryption to adequately protect electronic protected health information (ePHI).

• Systems providing public access should have an interface front end placed in the Demilitarized Zone (DMZ). If authentication to the system is required, then such authentication should be encrypted. The back end system will be placed on the appropriate segment of the network. A Virtual Private Solution (VPN) should be deployed if the system is being accessed by a third party vendor.

Other Requirements
• Test functions should be kept either physically or logically separate from production functions.

• Where appropriate, identification logon banners shall have warning statements that include the following topics: (1) unauthorized use is prohibited, (2) usage may be subject to security testing and monitoring, (3) misuse is subject to criminal prosecution; and (4) no expectation of privacy except as otherwise provided by applicable privacy laws.
• A risk analysis shall be conducted prior to rollout of a solution to determine the level of security that needs to be implemented to protect the information as required by policy or statutory regulations. The assessment should address the confidentiality, integrity and availability of the information. The implementation of controls used to mitigate identified risks should be appropriate and cost effective.

• Systems must be deployed in an area where adequate limited access controls are maintained and monitored.

• Where technically feasible, applications and directories are required to be connected to the M. D. Anderson’s deployed identity management infrastructure.

• Implementation of systems solutions must accommodate required application availability, dependencies with other systems, as well as requirements for data recovery, physical access and disaster recovery, in a manner that complies with all institutional, state and federal mandates.

• End user interfaces must comply with accessibility standards, guidelines and regulations.

• Systems that process, transmit or store cardholder data must comply with all Payment Card Industry (PCI) standards and regulations.

• Systems that maintain, transmit or store Social Security Numbers must comply with Policy #166 of The University of Texas System Administration Policy Library, available online at http://www.utsystem.edu/policy/ov/uts166.html.

• Systems that maintain, transmit or store digital research data must comply with Policy 167 of The University of Texas System Administration Policy Library, available online at http://www.utsystem.edu/policy/ov/uts167.html

**Additional Information about the Current Systems Environment**

**Attachments**

• M. D. Anderson Information Technology Standards