RIDER 114
NETWORK CONNECTIONS

1. Definitions.

Information Resources means any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDAs), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, Information Resources includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Network Connection means a connection that Contractor will use to access certain Information Resources on the MD Anderson network from an external network.

Protected health information (PHI) means individually identifiable health information as defined in 45 C.F.R. §160.103), as such provision may be amended.

2. Contractor Network Connections Requests and Approvals

A. All Contractor requests for a Network Connection must have MD Anderson's Information Security Department approval. Requests to Information Security for Network Connections must be accompanied by a completed **Contractor Network Connection Request-Information Requirements Document (the "Requirements Document");** a blank copy of the Requirements Document is attached as Attachment 1. This Requirements Document should be completed by the MD Anderson Sponsor requesting the Network Connection on behalf of the Contractor. It is the Contractor's responsibility to ensure that Contractor has provided all of the necessary information required for the MD Anderson Sponsor to complete the Requirements Document and that such information is correctly recorded in the Requirements Document submitted by Contractor.

B. All Contractors requesting a Network Connection must also complete and sign an MD Anderson Information Resources Acceptable Use Agreement and User Acknowledgement. The MD Anderson Information Resources Acceptable Use Agreement and User Acknowledgement must be signed by a Contractor representative authorized to bind Contractor and also shall be signed individually by each Contractor personnel who comes into MD Anderson facilities.

C. All Contractors requesting access to protected health information will be required to execute MD Anderson's standard Business Associate Agreement.

3. Connectivity Options

The following connectivity options are the standard methods for MD Anderson to provide a Network Connection. Any Contractor that wants MD Anderson to provide a Network Connection that deviates from the following standard methods must obtain a signed waiver from MD Anderson's Information Security Department.

A. Vendor Remote Access Solution – A remote access control solution for Contractors supporting systems on MD Anderson's network, and designed specifically for managing remote support. Contractor personnel will be enrolled and tied to their individual corporate email address for audit and access control.

B. Encrypted Tunnel - Encrypted tunnels should be terminated on the Contractor's network whenever possible. In certain circumstances, with the advance approval of MD Anderson's Information Security Department, it may be necessary to terminate an encrypted tunnel on a dirty subnet, in which case MD Anderson perimeter security measures will control access to MD Anderson internal devices.

C. Leased line/Circuit (e.g. T1, Frame Relay, etc.) - Leased lines should be terminated on the Contractor's network whenever possible. In certain circumstances, with the approval of MD Anderson's Information Security Department, it may be necessary to terminate a Leased Line/Circuit on a dirty subnet, in which case MD Anderson perimeter security measures will control access to MD Anderson internal

access.

D. Contractor may use modem connectivity only after obtaining the advance review and approval of the MD Anderson Information Security Department. Modem connection is an option of last resort that may be used only if other options are not feasible.

4. Network Security.

A. Contractor will be responsible for the selection, implementation, and maintenance of security technologies, procedures and policies that are sufficient to ensure that (a) Contractor's use of the Network Connection and Contractor's use of MD Anderson information resources is secure and is used only for authorized purposes, and (b) Contractor's business records and data are protected against improper access, use, loss, alteration or destruction.

B. Contractor will allow only specifically designated employees, subcontractors, agents of Contractor, or other persons for whom Contractor is responsible ("Workforce Members") to access the Network Connection or any MD Anderson Information Resources. Contractor shall be solely responsible for ensuring that authorized Workforce Members are not security risks. Upon MD Anderson's request, Contractor will provide MD Anderson with any information reasonably necessary for MD Anderson to evaluate security issues relating to any authorized Workforce Member's access to the Network Connection or any MD Anderson Information Resources.

5. Contractor Access Monitoring

Contractor is responsible for tracking and auditing its Workforce Members' access to MD Anderson Information Resources over the Network Connection and must be able to track activity back to an individual Workforce Member. Contractor will, upon request, provide MD Anderson with accounting of each individual Workforce Member who has accessed MD Anderson Information Resources. The retention periods for this tracking information are based on the classification of data available in the Information Resources being accessed, according to the following Data Classification Guidelines and Ratings. The data owner at MD Anderson will make the determination as to the Data Classification.

Data Classification Guidelines and Ratings

Data Classification	Definition	Criteria	Data Examples	Rating	Minimum Retention Period*
Public	Information obtained from the public domain or released to the public through official channels. All data not classified in one of the three categories below, falls into the public designation by default.	Negligible adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	De-identified, Aggregated Published Subject Data	1 User Authentication is not Required	60 days
Internal Use	Information intended to be generally releasable and used within MD Anderson, but should not be released to the general public.	Minimal adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	General policies/procedures, Employee phone list	2 User Authentication maybe required	60 days
Confidential	Information that, if compromised, would have a significant financial impact to MD Anderson, and violate federal or state law. Information that should be accessed only by a limited group of people. All data sets that contain PHI** receive this classification level, at a minimum.	Adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	Policies/procedures governing PHI. Financial, PHI, Proprietary, Research Protocols, Sensitive Research Data, Student Data.	3 User Authentication is Required	PHI for 6 years. Non-PHI for 1 year. Payment Card data for 1 year and 3 months online***
Restricted Confidential	Restricted Confidential builds upon the Confidential classification by addressing special access needs of a subset of PHI, such as mental health data. Restricted Confidential information should be accessed only by specific authorized people. Only the owner of the data may designate information sets as Restricted Confidential or grant access to this data.	Significant adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	Mental health, HIV, Genomics, Research Protocols Subject Data	4 User Authentication is Required	PHI for 6 years Non-PHI for 1 year

*Data owners set the retention schedule based on business needs as well as regulatory requirements. See also Records Management Policy IV.A.9.02
**Protected Health Information (PHI)
***Payment Card Industry (PCI) Sensitive Authentication Data must not be stored subsequent to authorization (even if encrypted)

6. Account Management.

Contractor shall notify the MD Anderson Sponsor responsible for requesting Contractor's Network Connection promptly upon the termination or change of role of any Workforce Member with an individual MD Anderson access account to the Network Connection. The MD Anderson Sponsor is responsible for notifying the appropriate MD Anderson Account Administrator to modify or revoke that Workforce Member's access. Generic contractor accounts will have a limited life of 90 days and will be terminated by MD Anderson at the end of this period. To re-initiate a generic contractor account, a Contractor will need to re-perform the routine account request process set forth in Section 2.

7. Services Provided

Services provided over Network Connections will be limited only to those services and those devices (hosts, routers, etc.) that are (i) explicitly set forth in the Agreement to which this Rider is attached or which MD Anderson determines that Contractor needs to access in order to provide the goods and/or services set forth in that Agreement and (ii) approved in advance by MD Anderson pursuant to the established procedures and the business purposes outlined by this Rider and the **Request Document**. MD Anderson will not provide **blanket access for Contractor, its Workforce Members, or anyone else.** Under no circumstances shall Contractor or any of its Workforce Members use a Network Connection to MD Anderson the Internet connection for the Contractor or the Workforce Members.

8. Contractor Equipment at MD Anderson Site

The Contractor will inventory and identify to MD Anderson all equipment owned or leased and maintained by Contractor that will be located on MD Anderson's facilities or premises ("Contractor Equipment.") Contractor is responsible for maintaining an inventory of all such Contractor Equipment, including but not limited to hardware, software, workstation, and peripheral devices included in such Contractor Equipment.

9. Protection of MD Anderson Confidential Information and Resources

A. Contractor must establish access Control on the Contractor's gateway to which the Contractor sites are connected. The access control will restrict access from predefined hosts within the Contractor's network to pre-defined hosts within the internal MD Anderson network. The access control will be determined by the business requirements as documented in the Requirements Documents; please refer to Attachment 1.

B. MD Anderson shall not be responsible for protecting Contractor's information, business records, data, networks (including Contractor's private internal network), or any Contractor Equipment. The Contractor shall be entirely responsible for providing the appropriate security measures to ensure protection of its network (including its private internal network), information, business records, data, and Contractor Equipment.

10. Audit and Review of Contractor Network Connections

Contractors shall be responsible for periodic reviewing of its audit logs of its and its Workforce Members use of the Network Connection and for immediately communicating to MD Anderson any potential compromise or misuse of the Network Connection.

11. MD Anderson Information Security Department

MD Anderson's Information Security Department is responsible for maintaining policies and standards related to Network Connections. Contractor will at all times comply with such policies and standards. The Information Security Department is responsible for the review and approval of all Network Connections.

12. Payment of Costs.

Contractor will be responsible for all costs incurred by Contractor related to implementing and maintaining a Network Connection, including, without limitation, costs for phone charges, telecommunications equipment, and for all personnel needed for maintaining the Network Connection.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf effective as of _____.

(Contractor)	MD Anderson
_____	_____
Authorized Signature	Authorized Signature
Name:_____	Name: _____
Title:_____	Title: _____
Date:_____	Date: _____

Attachment 1

CONTRACTOR NETWORK CONNECTIONS REQUEST - INFORMATION REQUIREMENTS DOCUMENT

Please submit completed form to MD Anderson's Information Security Department. If you have any questions about this document, please call 713-745-9000)

Project Name	**Overview/Purpose:** Please describe the nature of the request and its function in detail. *What is the desired end result? Must include a statement about the business needs of the proposed Network Connection.*

Scope of Needs:
What services are needed?
What are the privacy requirements (i.e. do you need encryption)?
What are the bandwidth needs?
How long is the Network Connection needed?

Type of Work:
What type of work will be done over the Network Connection?
What applications will be used?
What type of data transfers will be done?
How many files are involved?
What are the estimated hours of use each week? What are peak hours?

Type of Data:			
Check the classification of the data to be accessed according to the Data Classification Guidelines & Ratings and indicate the retention period as appropriate:			
Public	Internal Use	Confidential	Restricted Confidential
Days/Years	Days/Years	Years	Years

Miscellaneous:
Are there any known issues such as special services that are required? Are there any concerns or issues that you are uncertain about?
Is a backup Network Connection needed? (e.g., Are there any critical business needs associated with this Network Connection?)
What is the requested installation date? (Minimum lead-time is 60 days)
What is the approximate duration of this Agreement?
Will the Contractor be accessing PHI? If so, have they completed a Business Associate Agreement?
Has an Information Resources Acceptable Use Agreement and User Acknowledgement been signed with the Contractor and/or the appropriate workforce members of the Contractor?
Are there any existing Network Connections at MD Anderson with this Contractor?

Other useful information

Requestor Information: Please indicate the name of the responsible M D. Anderson Sponsor			
Contact	**Name**	**Phone Number**	**Web/Email Address**
Business Owner			
Manager			
Director			

Contractor Information: Please provide the points of contact for members utilizing this network connection. If it is not feasible to list the names of all workforce members, then provide a count of the approximate number of workforce members who will be using the Network Connection.
Name
Address
Host/domain names
Main Phone Number
Technical Support Hours

User/Escalation List			
Name	**Position**	**Phone Number**	**Web/Email Address**

Contact Information			
Contact	**Name**	**Phone Number**	**Email Address**
MD ACC Technical Contact			
MD ACC InfoSec Consultant			
Contractor Technical Contact			

System Information			
Source IP Address or Name	**Destination IP Address or Name**	**Service Port Number or Name**	**Protocol**