University of Chicago Medical Center

Request for Information - Business Partner

The requested information in this document must be completed by the Business Partner and returned to the appropriate University of Chicago Medical Center Project Manager, Business Analyst or Business Unit representative.

The following sections are provided in this document:

I. Medical Center Contact Information
II. Business Partner Contact Information
III. Business Partner Survey
IV. Technical Information

I. Medical Center Contact Information

Medical Center	
	Mailing Address
Company	University of Chicago Medical Center
Address	7955 South Cass
City/State	Darien, IL
Zip	60561
Medical Center Contact Information	
Helpdesk Phone	1-773-702-3456
Helpdesk Email	helpdesk@uchospitals.edu
Network Team email	networking@uchospitals.edu
Network Team page	1-773-753-1880 - page#1401
IT Risk and Security email	itrs@uchospitals.edu
IT Risk and Security page	1-773-753-1880 - page #1411

II. Business Partner Contact Information

The Business Partner should complete the following table:

Business Partner	
	Mailing Address
Company	
Address	
City/State	
Zip	
Support Contact Information	
Helpdesk Phone	
Helpdesk Email	
Name of Technical Contact	
Name of Backup Technical Contact	
Technical Team Email	
Technical Team Phone Number	

III. Business Partner Survey

Any Business partner seeking to transfer or receive data electronically must complete the following survey. By asking these questions, we seek to perform our due diligence in assuring the secure transfer and storage of sensitive information as they pertain to both the regulations discussed in HIPAA as well as what we consider to be a good business practice. The following survey must be completed prior to establishing a vpn connection.

1. What operating systems and versions are used at your location?
   Workstations
   Servers

2. As a security measure, have all unnecessary services been removed/disabled from the server(s)?
   - ☐ Yes
   - ☐ No
   - ☐ Only workstations will use the vpn tunnel

3. Do you limit access to customer data using:
   - ☐ File System permissions
   - ☐ Secure passwords
   - ☐ Policies
   - ☐ Database Access Lists
   - ☐ Role-based security
   - ☐ Physical security controls

4. To protect against security vulnerabilities in an appliance or operating system, do you have a patch management process documented?

5. Are the system logs managed and reviewed on a routine basis?
   - ☐ Yes
   - ☐ No

6. How often do you do perform security audits on your systems (i.e. perimeter scan, penetration test, vulnerability scans)?

7. When a security audit is performed, is it
   - ☐ Host-based
   - ☐ Network level

8. Where are your servers located?
   - ☐ Inside your network
   - ☐ Hosted via a third party

9. Do you use any of the following to protect your devices?
   - ☐ Router ACL's
   - ☐ Intrusion Detection/Prevention Systems
   - ☐ Network Firewalls

10. Do you allow any clear text protocols for authentication to servers or to transmit sensitive data?
    - ☐ Yes
    - ☐ No

11. Describe your backup procedures for data (e.g. type of encryption, off-site arrangements…)?

University of Chicago Medical Center
Request for Information - Business Partner

IV. Technical Information

Technical Information		
	Medical Center	**Business Partner**
VPN Device	Cisco 3030 VPN Concentrator	
Vendor Model	3030	
Patch-FOS Level	4.7.2	
Technical Description	IPsec with IKE tunnel	
Mode	Tunnel mode	
Implementation	Site to Site	
Mode		
Tunnel Endpoint	165.68.16.22	
Direction of Tunnel	Bi-directional	
IP Encryption Domain (Identify networks or subnets)		
Host	Host	*Smaller network or ip address preferred*
Network	Network	
VPN Specifications		
IKE Phase 1 (ISAMKMP)		
Authentication	Pre-shared Key	
Encryption	3DES-168	
Hash Algorithm	MD5-HMAC-128	
Key Exchange	D-H Group 2	
Lifetime	IKE is 86400 Seconds	
IKE Phase 2 (IPSec)		
Protocol	ESP	
Encrypt	3DES	
Hash	MD5	
SA Lifetime	IPSec is 28800 seconds	
PFS	None	
Compression (LZS)	None	
Pre-shared Secret	A preshared key containing at least 12 characters, upper/lower case, numbers and special characters will be provided by the Medical Center	
IP Address and Port Information		
Notes: *Please include all source and destination IP addresses including which tcp or udp ports are needed.* *All Business Partner IP addresses must be routables, RFC 1918 address space is not permitted on the Medical Center network.*		
IP Address (source)	IP Address (destination)	Ports (tcp or udp)