

UNIVERSITY MEDICAL CENTER OF SOUTHERN NEVADA
RFP No. 2011-16
PCI Compliance Services

August 8, 2011

ADDENDUM NO. 2

QUESTIONS / ANSWERS

Payment Card Industry Data Security Standard (PCI DSS) Scoping Questions

<u>Questions</u>		<u>Answers</u>
<u>Acquiring Bank / Merchant Level</u>		
1.	Who is your acquiring bank?	Bank of America
2.	Have the number of individual merchant IDs been determined?	Unknown
3.	Has your merchant level been determined? If so, what is it?	Level 4 when last assessment performed, May 2008
4.	What is your compliance deadline given by your acquirer?	Unknown
5.	Have you had any incidents resulting in the compromise of cardholder data? If so, please describe the incident and any remedial actions?	No
<u>Cardholder Data Environment</u>		
5.	How many different ways do you accept credit cards (e.g., admitting, pharmacy, parking, gift shop, etc.)? Please describe and provide any available information.	UMC Cashier, Quick Care/Primary Care Clinics, Outpatient Pharmacy, Online Pharmacy Refill, Online Bill Pay, Online UMC Foundation Contributions, Cafeteria (vendor-run concession), Gift Shop (vendor-run concession)
6.	Have you defined your cardholder data environment? If so, please describe and provide any available information.	May 2008 assessment defined our card holder environment, changes made in the last three years has impacted that initial definition
7.	Do you store cardholder data?	Yes
8.	Is there any in-house developed software that processes credit card transactions?	Yes; however, the "processing" is somewhat indirect. Payment card information is collected through an online, home-grown customer interface and sent to our business office. The process of transmitting the payment is done manually by business office personnel through a POS system.
9.	Do you leverage any commercial payment applications from vendors? If so, how many? Are they PA DSS certified? Please provide any	No

	available information.	
10.	Do you leverage any PCI DSS certified service providers? If so, how many? Please provide any available information.	No
11.	Do you have a process flow for your authorization process? If so, please describe and provide any available information.	Revenue Cycle likely has a process; not familiar with details
12.	Do you have a process flow for your settlement process? If so, please describe and provide any available information.	Revenue Cycle likely has a process; not familiar with details
13.	Has any network segmentation been implemented to segment your cardholder data environment from the rest of the corporate network? If so, what has been implemented (VLAN, Firewall, etc.)?	It has been discussed but no actual segmentation has been implemented
14.	How many different Internet, DMZ, or segmentation firewalls are in place?	Two firewalls at the perimeter, DMZ is a leg off the firewall
IT Components		
15.	Please indicate approximately how many of the following constitute your cardholder data environment :	
a.	Physical buildings and locations	Approx. 15 (main campus, offsite clinics)
b.	Data Centers and locations	2 (main campus data center, co-location facility)
c.	Number of stores / restaurants / branches / distributed locations (as applicable)	Approx. 15-20 (main campus, offsite clinics, gift shop, cafeteria)
d.	Internet connections – locations and purpose	Two redundant, 100 Mb Internet connections to support all Internet-based production traffic; single 50 Mb guest wireless Internet connection to support patient, visitor traffic (physically separate from production circuits)
e.	Third party connections – number, entity, purpose, and type of connection (e.g., frame relay, VPN, etc.)	Approx. 120 VPNs (both site to site and client) implemented to facilitate vendor system/application support services, physician offices billing, accounts receivable billing and collections, clinical data sharing; unknown how many encompass cardholder environment
f.	Servers – number, operating systems	Total population approx. 300 (physical and virtual), majority run Windows 2003 or 2008, small number of UNIX boxes; unknown how many encompass cardholder environment
g.	Databases – number, vendor software, type of information stored.	Number unknown, Microsoft SQL 2003 and 2008; unknown how many encompass cardholder environment
h.	Routers and Switches – approximate number and vendor	220; network infrastructure is all Enterasys, perimeter firewalls are Checkpoint, VPN is Checkpoint

i.	Wireless Access Points – number, vendor, locations, purpose, encryption employed (e.g., none, WEP, WPA, WPA2), and authentication employed (e.g., shared key, LEAP, PEAP, etc.)	Approx. 320 APs, Enterasys devices (model unknown), WPA2, fairly certain authentication model is shared key
j.	Workstations – number locations, purpose, operating systems	Approx. 1,800; end user desktops, distributed throughout UMC enterprise, run Windows XP; unknown how many encompass cardholder environment
k.	Is Active Directory or LDAP in place? If not AD (and Group Policy), is there any type of centralized configuration control capability (e.g., ZenWorks).	Yes, Microsoft Active Directory infrastructure, domain controllers currently run Windows 2003
<u>Previous Compliance Validation</u>		
16.	Did you validate your compliance last year? If so, did you leverage a self assessment questionnaire or a Qualified Security Assessor (QSA) Report on Compliance (ROC)?	No, last assessment completed May 2008; no report or SAQ submitted to merchant bank
17.	With last year's compliance validation, did you need to leverage any compensating controls? If so, please provide the quantity and a brief description.	Not applicable

The RFP due date of **Tuesday, August 23, 2011 at 2:00:00 P.M.** remains the same. Should you have any questions, please contact me at (702) 207-8291 or via email at Rebekah.holder@umcsn.com.

Issued by:

Rebekah Holder
Sr. Contract Management Analyst
UMC