SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

September 12, 2011

ED BABAKANIAN
Chief Information Officer
8983

IRA GOODMAN
Associate Director, Administration
Moores Cancer Center
0658

TRISH LOLLO
Associate Administrator, Moores Cancer Center
0658

Subject: ***Cancer Center Data Security – Phase I Risk Assessment***
AMAS Project 2011-22

Audit & Management Advisory Services (AMAS) has completed a preliminary risk assessment of data security management processes and technologies implemented for selected Moores Cancer Center (MCC) networks. This report provides the results of our review.

Background

The Moores Cancer Center (MCC) is one of five UCSD School of Medicine (SOM) Organized Research Units (ORUs). Established in 1979, the MCC is one of 40 National Cancer Institute (NCI) designated Comprehensive Cancer Centers in the United States. MCC research laboratories and clinic facilities support cancer related research, clinical research projects, cancer prevention and outreach programs, and comprehensive clinical care.

The MCC network connects to the UCSD campus network backbone, and supports various types of hardware components, including servers, workstations and mobile devices. These devices are used to operate specialized software applications including operating systems, email, customized websites, word processing, spreadsheets, and internally developed systems. Network resources are managed by information technology administrators within individual MCC departments and research units, in coordination with campus Administrative Computing and Telecommunications (ACT) and UCSD Health System Information Services personnel.

MCC network security management is highly complex due to the distributed network management structure, and the division of responsibility for maintaining security between MCC departments and research units. AMAS identified five distinct MCC based networks, which were supported by the units noted below:

Department/Unit	***Operational Reporting Relationship***
UCSD Health System Information Systems (HSIS)	Chief Information Officer, UCSD Health Systems
Radiation Oncology (RO)	Director, RO Medical Physics
Bioinformatics/Biostatistics (A Cancer Center Shared Resource)	Cancer Center Shared Resources Oversight Committee
Chronic Lymphocytic Leukemia Research Consortium (CLL)	Principal Investigator, Core A Administrative Unit CLL
MCC Information Systems (MCC)	Associate Director, Administration MCC

With the increasing number of legislative requirements mandating the protection of personally identifiable information (PII) and protected health information (PHI), departments maintaining sensitive data must be particularly focused on ensuring that network security is adequate to comply with applicable regulations. Information residing on research computing equipment could include PII as defined by California State Bill 1386. Systems that store PHI are subject to Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements.

In addition to legislative requirements, MCC network equipment must also conform to University of California (UC) Business and Finance Bulletin IS-3 (IS3), *Electronic Information and Security Policy;* and UCSD Policy and Procedure Manual 135-3 (PPM 135-3), *Network Security*; and PPM 135-3 Exhibit C: *Minimum Network Connection Standards* (Minimum Standards). IS3 establishes guidelines for achieving appropriate protection for University electronic resources, and for identifying information security roles and responsibilities at all levels in the University of California system. PPM 153-3 Exhibit C standards provide minimal security requirements for devices that are connected to the UCSD Campus network backbone.

Audit Objectives, Scope and Procedures

The objectives of our review were to determine the type and amount of sensitive data stored on MCC clinical workstations and file servers; and to validate that minimum standard security measures have been implemented as designed.

We completed the following audit procedures to achieve project objectives:

- Reviewed PPM135-3;(Minimum Standards), and IS3;

- Obtained a detailed understanding of network security practices by collecting and analyzing responses to a Computer Environment Internal Control Questionnaire (ICQ) and the supporting documentation provided by the five MCC networks being assessed. The questionnaire covered the following network administration and security topics:

  - ✓ General Support (*number of users, computers, type of computing, etc.*)
  - ✓ System Configuration
  - ✓ Policies and Procedures
  - ✓ Adware/Spyware
  - ✓ Network Configurations
  - ✓ Router and Switches

- ✓ Firewalls
- ✓ Virus Protection/Detection
- ✓ SPAM[1]
- ✓ Logical Security
- ✓ Disaster Recovery
- ✓ Physical Security/Environmental Controls
- ✓ Software Licensing
- ✓ Application Development
- ✓ Incident Management
- ✓ Change Management
- ✓ Data Security;

- o Interviewed department and research unit network security staff to discuss the responses they provided on the questionnaire and obtain additional insight into security practices; and,

- o Completed a preliminary network security risk assessment based on elements of IS3, PPM 135-3 and the Minimum Standards (***Attachment A***).

Because the CLL was included within the scope of AMAS Project #2010-22, School of Medicine Web Application Security, it was not further evaluated during this project. Radiation Oncology operates two satellite facilities, one in Encinitas and the second in South Bay. The network that supports the South Bay facility was not evaluated within the scope of this review.

Conclusion

Based on our preliminary evaluation, we concluded that network security procedures and technologies in one MCC unit (HSIS) appeared adequate to comply with federal and state regulations and University policy. HSIS network security staff demonstrated a good understanding of IS3 and Minimum Standards requirements through their description of how computer resources within their purview are secured. However, information provided by the three other MCC units included in our review indicated that additional focused review would be required to verify that certain network security controls have been fully implemented.

Based on the responses provided in the ICQ and client interviews, AMAS prepared a risk assessment matrix (***Attachment A***) to ensure that network security risk was properly identified. We plan to complete a detailed review of network security controls for topics identified in the matrix with an "X" during Phase II of this project to determine whether security controls in place effectively mitigate identified risks. Focused audit testing will be completed to validate that the control procedures are operating as designed, and effective to mitigate the risk.

[1] The term SPAM is defined as the use of electronic messaging systems (including most digital delivery systems) to send unsolicited bulk messages indiscriminately.

Audit & Management Advisory Services appreciated the cooperation and assistance provided during this review. Because no audit recommendations have been included in this report, a management response is not required.

UC policy requires that all draft audit reports be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel or destroy them at this time.

If you have any questions regarding this report, please call me at 534-3617.

Stephanie Burke
Assistant Vice Chancellor
Audit & Management Advisory Services

cc: D. Brenner
R. Deteresa
R. Fletcher
T. Jackiewicz
G. Matthews
K. Messer
T. Perez
M. Sonnenshein
S. Vacca
K. Wottge

Cancer Center Data Security
Audit & Management Advisory Services Project 2011-22
Risk Assessment Matrix - Attachment A

		Preliminary Status			
Assessment Categories	**Objective**	**Radiation Oncology**	**Moores Cancer Center**	**Bioinformatics/ Biostatistics**	**Medical Center Clinical Enterprise**
Management Measures: People					
1. Security Education and Awareness Training	Assess employee's awareness of System-wide Security policies.	X	✓	X	✓
Management Measures: Processes					
2. Asset Inventory and Classification	Assess the process for identifying electronic information resources and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources.	✓	X	✓	✓
3. Risk Assessment	Assess the process to understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources. Identify the level of security necessary for the protection of the resources.	X	X	✓	✓
4. Information Security Plan	Assess the departments documented process for accepting a level of risk for systems and processes, and that procedures and controls in place will enhance the security of information assets.	X	✓	✓	✓
5. Workforce Administrative	Assess the process for granting and/or revoking, authorizing and protecting access to information systems.	✓	✓	✓	✓
6. Physical/Environmental Controls	Assess the procedures for physical protection of resources that support restricted or essential systems and/or data.	✓	✓	✓	✓
7. Incident Response Planning and Notification Procedures	Assess the process for reporting and handling a security incident.	✓	X	X	✓

X = Risk level warrants further assessment of compensating controls.

✓ = Initial assessment indicated low risk level which may be adjusted as appropriate during Phase II.

Cancer Center Data Security
Audit & Management Advisory Services Project 2011-22
Risk Assessment Matrix - Attachment A

Assessment Categories	Objective	Preliminary Status			
		Radiation Oncology	**Moores Cancer Center**	**Bioinformatics/ Biostatistics**	**Medical Center Clinical Enterprise**
Technical Measures					
8. Identity and Access Management	Assess the technical measures for controlling authentication and authorization (password policy, access rights/roles).	✓	X	X	✓
9. Access Controls to Authenticate and Authorize Users	Assess the controls for session protection, automatic logout, and procedures for managing privileged accounts.	✓	✓	✓	✓
10. Systems and Applications Security	Assess the procedures in place for systems responsibilities including separation of duties; backup and retention efforts; and patch management practices.	X	✓	X	✓
11. Application Systems Management	Assess the process for application version control and migration practices from development to quality assurance to the production environment. Assess the change management practices for software development and configuration.	X	X	X	**N/A**
12. Collection, Management and Analysis of Log Data	Assess the audit log infrastructure and review practices.	✓	✓	X	✓
13. Data Protection and Encryption	Assess the use of encryption for data in transit and data at rest.	X	X	X	✓
14. Risk Mitigation Measures	Assess the process for prevention, detection, and recovery from emergency conditions.	✓	X	X	✓
15. Network Security Tools and Practices	Assess network security strategies and technical security measures (Minimum Requirements for Network Connectivity).	X	X	X	✓

X = Risk level warrants further assessment of compensating controls.

✓ = Initial assessment indicated low risk level which may be adjusted as appropriate during Phase II.