15-404 Pinnacle Application Assessment

EXECUTIVE SUMMARY

Pinnacle is the primary radiation treatment planning application operated on more than 80 workstations. The application helps streamline radiation therapy planning through advantages in processing speed and increased access to data throughout the enterprise to expedite plan completion and approval.

Pinnacle is critical to patient care, and downtime would impact the ability to provide services to patients in a timely manner. This application stores and processes confidential patient health information and is utilized primarily by the Radiation Oncology department with approximately 300 users. The Radiation Oncology Information Systems team functions as part of the centralized Institutional Information Services and provides functional IT support both within the department and within central IS, including issue and problem management, user security access provisioning, patient data backups, and moving changes to the production environment. Additionally, Pinnacle is supported by a third party vendor (Phillips Healthcare) who provides technical support by providing end-user trouble shooting and performing program change / development activities (updates, patches, hot fixes).

Audit Results Summary:
Radiation Oncology IS has a strong control environment with many control processes related to security, operations, changes and system development. Although we noted many effective control processes in place to manage Pinnacle, we noted the following opportunities for improvement:

- Management should implement a formal process where all issues and problems/troubleshooting are captured within a Cherwell ticket and significant incidents are escalated to Information Security.
- Management should design and implement periodic user access recertification and review controls in order to ensure that inappropriate access is being identified and removed on a timely basis.

Management Summary Response:
Management’s action plans have been developed by the Pinnacle team. The action plans that follow will be completed by January 1, 2016.

Number of Priority Findings to be monitored by UT System: None
A Priority Finding is defined as “an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.”
The courtesy and cooperation extended by the Pinnacle team was sincerely appreciated.

Sherri Magnus, CPA, CIA, CFE, CRMA  
Vice President & Chief Audit Officer  
September 1, 2015
Observation 1: **Problem and Incident Management**

Internal Audit noted that management does not have formalized policies and procedures around the issue and problem management/troubleshooting process. An informal process is in place where users notify the RadOnc IS analyst via email, phone for any front-end application issues. All significant backend system issues are reported to the institution's centralized Information Security function via Cherwell. However, no policies and procedures exist to identify and classify incidents. This increases the risk that problems or issues with the application or server are not resolved in a timely manner, and increases the risk that significant events are not identified and escalated appropriately. A formal and defined issue and problem management/troubleshooting process allows the institution to manage, track, and escalate issues timely.

**Recommendation:**

Management should develop and document policies and procedures over the issue and problem management/troubleshooting process. This will help end-users identify and classify types of issues/problems/troubleshooting events and the appropriate method of reporting to resolve the issue. Additionally, management should implement a process to track and retain documentation of all reported frontend application issues and resolutions.

**Management's Action Plan:**

Responsible EVP: Leon Leach
Owner: Peter Balter, Ph.D.
Due Date: January 1, 2016

*We will update our Pinnacle support procedures to reflect that issues are clinical, IT, or patient safety. We will continue to use immediate on-line support for the clinical support issues for which no tickets need to be generated. We will continue to use the Cherwell ticket system for any issue that requires support from the Rad-Onc IT team, we will continue to use our incident learning system and direct contact with the manufacturer for any patient safety related issue.*

Observation 2: **User Access Reviews**

Internal Audit noted that management does not have a formal user access recertification process for the Pinnacle application. The termination process is relied on to remove inappropriate access as the application authenticates through the active directory process. However, this does not cover users that have transferred or changed job roles and no longer require access to the application. This increases the risk that a terminated and/or transferred employee may have inappropriate access to the application. The institutional information security policy outlines that all user access should be reviewed periodically by the appropriate management personnel.

**Recommendation:**

Management should implement independent user access reviews performed on a periodic basis. Management should implement formal procedures to retain user access review, approval, and follow-up documentation.

Please note that this document contains information that may be confidential and/or exempt from public disclosure under the Texas Public Information Act. Before responding to requests for information or providing copies of these documents to external requestors pursuant to a Public Information Act or similar request, please contact the University of Texas MD Anderson Cancer Center Internal Audit Department.
We will implement a procedure for user recertification based on automatic validation of AD group membership vs job title. For all users in job titles that require Pinnacle access in order for them to accomplish their daily work the recertification shall be automatic. For those in job titles that do not require this access their supervisor will be emailed for validation that they still need access. This will be done annually. We will continue to rely on the institutional exiting process for users that leave the institution. These audits will be in place by the end of 2015.
Appendix A

Strategic Area: Information Technology, Information Security, Pinnacle
Risk Type: Compliance and Operational

Objective, Scope and Methodology:

The objective of this project is to evaluate controls over Pinnacle, a tier two application, including information technology general controls related to restricted access and program change management, the annual risk assessment, report integrity, and interfaces.

The scope of this internal audit is focused on the execution of controls in MD Anderson’s environment and to evaluate controls over Pinnacle including information technology general controls related to the risk assessment, restricted access, program change management, interfaces, and report integrity. Our testing period of coverage was from 9/1/2014 to 5/31/2015.

Our procedures included the following:

• Interviewed key personnel within the Radiation Oncology IS team for the Pinnacle application.
• Gained an understanding of Institutional Policies and Procedures and compared to Pinnacle current control environment for the following areas:
  ➢ Risk Assessment
  ➢ Security
  ➢ Change Management
  ➢ Computer Operations
  ➢ Issue and Problem Management

Our internal audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

Please note that this document contains information that may be confidential and/or exempt from public disclosure under the Texas Public Information Act. Before responding to requests for information or providing copies of these documents to external requestors pursuant to a Public Information Act or similar request, please contact the University of Texas MD Anderson Cancer Center Internal Audit Department.