

## 17-206 Sunrise Clinical Manager

We have completed our audit of the Sunrise Clinical Manager application. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

### BACKGROUND

Sunrise Clinical Manager (SCM) is a comprehensive electronic health record system implemented at UTHealth Harris County Psychiatric Center (HCPC) in 2001. SCM allows for secure access to patient records and streamlines the documentation, assessment, and management of patient care. SCM interfaces with Invision for accounting, patient registration, and patient discharge/transfer. Prescription and dosage information is printed from SCM for transcription into Medics.

### OBJECTIVES

The objective of this audit was to determine whether controls over the Sunrise Clinical Manager application are adequate and functioning as intended.

### SCOPE PERIOD

The scope period was October 1, 2016 – September 30, 2017.

### METHODOLOGY

The following procedures were performed:

- Obtained list of active SCM users and reviewed appropriateness of access and synchronization to Active Directory (AD) user credentials. Selected a sample of active users and verified Management Information System Service Requests (MSRs) were submitted and approved. Selected a sample of guest accounts and reviewed completion of guest account forms and approval by appropriate supervisors.
- Reviewed and verified most recent quarterly review of access listings was completed. Obtained evidence that users cannot access VIP patient records and reviewed session timeout settings.
- Verified SCM policies and procedures exist. Obtained evidence mandatory input fields in SCM display warnings for incomplete fields or do not allow for continuation without completion. Reviewed patient photography process for proper deletion of patient images. Verified patches, vendor contracts, and service level agreements are current and up-to-date.
- Obtained results of the most recent disaster recovery test and assessed for reasonableness and accuracy. Verified Continuity of Operations Plan is up-to-date. Reviewed documentation of SCM downtimes/outages and verified root cause analysis was performed and sufficient resolution was reached. Verified no information security incidents were reported during the audit period.

**17-206 Sunrise Clinical Manager**

**AUDIT RESULTS**

A&AS identified areas of improvement related to patient images, session lockout settings, and application access:

- Patient images are not deleted on a timely basis from Admissions PCs and portable digital cameras.
- The SCM session lockout settings are not correctly documented.
- Six individuals remained active in SCM even though access to AD had been removed.

**NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM**

None

We would like to thank the staff and management within the HCPC MIS, Information Technology, and IT Security departments who assisted us during our review.



\_\_\_\_\_  
Brook Syers, CPA, CIA, CFE, CISA  
Senior Audit Manager, I.T.

**MAPPING TO FY 2017 RISK ASSESSMENT**

<b>Risk (Rating)</b>	R.27 An E.H.R application utilized by UTH is not secure. (High)
----------------------	---

**DATA ANALYTICS UTILIZED**

<b>Data Analytic #1</b>	Compared active SCM user credentials to AD to detect unauthorized users and verify synchronization.
-------------------------	---

**AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM**

<b>Audit Manager</b>	Brook Syers, CPA, CIA, CFE, CISA
<b>Auditor Assigned</b>	Tammy Tran, CISA
<b>End of Fieldwork Date</b>	November 17, 2017
<b>Issue Date</b>	December 12, 2017

**Copies to:**

Audit Committee  
Richard Miller  
Dr. James Griffiths  
Stephen Glazier  
Lois Pierson  
Dr. Melissa Allen  
Carina Ayers  
Chioma Odili

<p><b>Issue #1</b></p>	<p>The <i>HCPC MIS Patient Photography and Recording Security Policy</i> states that patient images are captured by Admissions staff and temporarily stored to the C:\PatientPhotos folder. After uploading the images to SCM, Admissions staff delete them from the folder. Additionally, a script runs on a nightly basis to delete any images from the C:\PatientPhotos folder on all Admissions PCs.</p> <p>A&amp;AS spoke with various Admissions staff concerning the patient photography process. We randomly selected an Admissions PC and noted the following:</p> <ul style="list-style-type: none"> <li>• The script was not installed on this PC.</li> <li>• Images from a previous month were noted in the local Pictures folder.</li> </ul> <p>Additionally, staff members stated a portable digital camera is used to record patient images in other areas of HCPC. A staff member advised the images on the camera are deleted daily; however, on the date of our walkthrough, images from the previous day were present on the digital camera.</p>
<p><b>Recommendation #1</b></p>	<p>We recommend management develop a process to ensure all images are removed from Admissions PCs on a nightly basis. Additionally, we recommend training be provided to Admissions staff to ensure images are deleted from the digital camera on a daily basis.</p>
<p><b>Rating</b></p>	<p>Medium</p>
<p><b>Management Response</b></p>	<p>The System Center Configuration Manager profile for all Admissions PCs has been updated to include a script that removes all .jpg file extension objects from the C:\PatientPhotos folder on a nightly basis.</p> <p>MIS will perform quarterly spot checks to ensure the script is installed and running as expected.</p> <p>As a part of the Quarterly User Audit, Admissions staff will be educated on the policy and procedure for managing patient photos, including deleting all photos before and after taking new photos and saving photos to the C:\PatientPhotos folder.</p>
<p><b>Responsible Party</b></p>	<p>Dr. James J. Griffiths, Executive Director &amp; Clinical Technology Officer</p>
<p><b>Implementation Date</b></p>	<p>Implemented as of November 20, 2017 (To be verified by A&amp;AS prior to the next Audit Committee meeting)</p>

## 17-206 Sunrise Clinical Manager

<b>Issue #2</b>	<p>The <i>HCPC MIS Sunrise Clinical System Auditing Policy</i> states SCM sessions are suspended after 30 minutes of inactivity and locked after 40 minutes of inactivity.</p> <p>A&amp;AS confirmed during a walkthrough that SCM sessions are locked after 60 minutes of inactivity, with users receiving a warning two minutes prior to the lockout.</p>
<b>Recommendation #2</b>	We recommend management update the <i>HCPC MIS Sunrise Clinical System Auditing Policy</i> to reflect the correct session lockout settings.
<b>Rating</b>	Medium
<b>Management Response</b>	The <i>HCPC MIS Sunrise Clinical System Auditing Policy</i> has been updated to reflect the 60-minute timeout and 2-minute warning.
<b>Responsible Party</b>	Dr. James J. Griffiths, Executive Director & Clinical Technology Officer
<b>Implementation Date</b>	Implemented as of November 6, 2017 (Verified by A&AS prior to issuing the report)

17-206 Sunrise Clinical Manager

<b>Issue #3</b>	<p>The <i>HCPC MIS Sunrise Clinical System Auditing Policy</i> states SCM credentials are synchronized to AD and access is disabled upon termination of employment. To access SCM, individuals must have access to both AD and SCM.</p> <p>A&amp;AS obtained a list of all active users in SCM and verified synchronization with AD. Of the 1,209 active SCM users, 6 remained active in SCM even though their access to AD had been removed. Access approvers did not request removal of access during the most recent quarterly review.</p>
<b>Recommendation #3</b>	<p>We recommend MIS remove SCM access for individuals with inappropriate access. Additionally, we recommend reemphasizing the importance of the quarterly access reviews to access approvers to ensure individuals with inappropriate access are removed.</p>
<b>Rating</b>	<p>Medium</p>
<b>Management Response</b>	<p>Access was removed for the six users on November 22, 2017.</p> <p>The following phrase has been added to all Quarterly User Audit emails: <i>“REVIEW LISTS CAREFULLY FOR ANY ACCESS THAT SHOULD BE ENDED – this is a critical audit function!”</i></p> <p>HCPC’s Chief Medical Officer has developed an exit document to include notification to MIS of faculty termination so SCM access can be removed.</p> <p>MIS will run a LDAP query (created by the IDM team) that will return a list of all inactive residency training group users (with user ID and expiry timestamp) that went inactive during a defined date range. MIS will run the query weekly and remove SCM access as needed.</p>
<b>Responsible Party</b>	<p>Dr. James J. Griffiths, Executive Director &amp; Clinical Technology Officer</p>
<b>Implementation Date</b>	<p>February 1, 2018</p>