

Security Efforts for SEER*DMS

SCOTT DEPUY & LINDA COYLE – IMS, INC.

2018 SEER*DMS MEETING

SEPTEMBER 26, 2018

Penetration Testing

Conducting a pentest is the practice of systematically testing a computer system, network, or web application to find vulnerabilities that an adversary could exploit.

These will continue to be conducted annually by an independent organization.

Independent Penetration Tests

Test #1: August 2016

- Coalfire (www.coalfire.com)
- Squish #4984

Test #2: January 22 – February 2, 2018

- Lunarline (www.lunarline.com)
- Squish #6008

2018 Penetration Test

Credentials provided (white box) for:

- SEER*DMS – with a special focus on:
 - Limited access users submitting an import file
 - File transfer utility
- SEER*Stat

No credentials (black box):

- PostgreSQL
- SSH (auto-loading)

Application Vulnerability Scans

Conducted quarterly by the IMS Security and Compliance Team. This team works independently from the SEER*DMS developers, system administrators, and DBAs.

Tools:

- Burp Suite (www.portswigger.net/burp)
- Acunetix (www.acunetix.com)

These are different than the automated system and network scans for which execute weekly via a tool named Nessus.

Incident Response Drill

Conducted annually and facilitated by the IMS Security and Compliance Team.

- Conducted on July 31, 2018
- The drill simulated the compromise of the SEER*DMS system via a rogue account.
- It was a table top exercise that did not involve actual systems.
- The role playing confirmed whether responsible staff knew the correct SOPs to follow.
- It also confirmed that staff were able to correctly interpret the directions within the SOPs.
- The drill could expose deficiencies in IMS's SOPs.

Incident Response Drill – Scenario

A suspicious user account was discovered during a routine SEER*DMS account audit. It was also determined that the rogue account has data access privileges and was created by a user that should not have had sufficient permission to create the account. The rogue account was used to access sensitive data. It is possible that the rogue account was utilized to download sensitive data in addition to merely being a means of viewing it. The misconfiguration of a user account was the precursor to the creation of the rogue account. The possibility exists that other accounts could also be misconfigured...

Incident Response Drill – Lessons Learned

- Additional detailed logging of user actions within SEER*DMS should be explored.
- IMS's SOPs should specifically discuss evidence preservation for potential follow-up investigations.
- IMS's SOP0405 for Network/Computer Incident Response was generally sufficient, however some improvements in the decision tree and role definitions should be considered.

AICPA System and Organization Controls

Similar in nature to the NIST Risk Management Framework

Defined by the American Institute of Certified Public Accounts

- SOC 1 – financial reporting controls
- SOC 2 – data security
- SOC 3 – simplified SOC 2 requiring less formalized documentation
- Type 1 – control demonstrated for a point in time
- Type 2 – control over a period of time (typically 1 year)

SOC 2 Type 2 reports are useful when considering vendors for managed IT services. A company that has achieved this certification has proven its system is designed to keep its clients' sensitive data secure.

SOC 2 Type 2 – Trust Service Principles

NIST Risk Management Framework

- Confidentiality
- Integrity
- Availability

SOC 2 Type 2

- **Security**
- Availability
- Processing integrity
- **Confidentiality**
- Privacy

Why both for SEER*DMS?

- Not all organizations are familiar with federal government standards. The Mayo Clinic would only accept SOC 2 reports for the continued delivery of data for Iowa residents.

SOC 2 Type 2 - Readiness Assessment

A readiness assessment is designed to assist a service organization in assessing their preparedness for a formal SOC engagement.

IMS was engaged with Schellman (www.schellman.com) from November 2017 – March 2018.

Readiness assessment report was provided to the NCI.

Control activities insufficient to meet trust services criterion:

- Background checks are not performed for employees as a component of the hiring process.
- A holistic risk assessment is not performed at least annually with consideration of the following components...

SOC 2 Type 2 – First Annual Term

June 1, 2018 – May 31, 2019

Schedule:

- April 12, 2019: Schellman provides IMS with the project plan and the first information request list
- May 12, 2019: IMS's first response and set of evidence is due
- May 12 – 23, 2019: Schellman's on-site field work
- June 14, 2019: first draft report due to IMS

NIST Risk Management Framework

Additional Plans for 2019:

- Quarter 2: Independent Assessment
- Quarter 3: IMS Response via Plan of Action and Milestones (POA&M)
- Quarter 4: NCI Consideration for an Authority to Operate (ATO)

SEER*DMS: Security Related Changes

PRACTICAL APPLICATION OF FINDINGS FROM SEER*DMS SECURITY
AUDITS AND TESTING

SEER*DMS Security – Related Activities

Security is a responsibility shared by IMS and registry staff.

IMS implemented several changes in response to findings from the SOC-2 Readiness Assessment, Incident Response Drill, Penetration Testing, and Vulnerability Scans.

These included changes to IMS processes and changes to SEER*DMS itself. These were mostly “under-the-hood” changes that could not be detected by SEER*DMS users. A few changes did affect SEER*DMS users.

IMS believes it is important for registry staff to understand our dedication to maintaining security of your registry’s data and system; and we believe it is important for all registry staff to join us as motivated teammates in these efforts.

Security Audits & System Changes

- ❖ **Audits of SEER*DMS login accounts and VPN credentials**
 - ❖ IMS staff audit user accounts and VPN credentials in all SEER*DMS registries.
 - ❖ The audits are conducted every 6 months.
 - ❖ The registry manager or security officer is informed if there is an active account that has not been used in 6 months.
- ❖ **Added a feature in SEER*DMS to automatically deactivate unused accounts.**
 - ❖ Registry management is encouraged, but not forced, to take advantage of this feature.
 - ❖ An account is deactivated if the user has not logged in within an amount of time specified in the registry's configuration. Typical setting = 6 months, but some registry's parent institutions require a shorter period of time.

SEER*DMS Security Audits – PostgreSQL

❖ Audits of PostgreSQL login accounts

- ❖ PostgreSQL login accounts are available in some registries. These were created to support systems maintained by registry IT staff.
- ❖ IMS staff conduct an audit of registry PostgreSQL accounts every 6 months.
- ❖ Goals of this effort:
 - ❖ Minimize PostgreSQL accounts; remove all unnecessary accounts
 - ❖ Prohibit the use of shared Postgres accounts. In 2005, the practice was to create a single “admin” account that was shared by registry IT staff. These will be eliminated, if possible, in consultation with the registry or they will be converted to personal accounts.

SEER*DMS Security Audits – IMS Access

- ❖ **Audit IMS access to registry data and systems**

- ❖ IMS systems team and project managers conduct a review of IMS access to registry islands. This audit is conducted every 6 months.
- ❖ Access is provided to specific IMS staff based on static IP addresses.
- ❖ First, a system administrator reviews all IP addresses and creates a list of IMS staff and their level of access.
- ❖ Two project managers review and confirm the list:
 - ❖ Nicki Schussler – verifies that current, signed data use agreements are in place
 - ❖ Linda Coyle or Chuck May – review the list to verify that all staff are active members of the development team; and that the level of access is appropriate

SEER*DMS Security – Related Changes

- ❖ **Implemented a new framework to track security related events. This system tracks events that impact data usage and system security. The initial version includes these events:**
 - ❖ Login attempts
 - ❖ Changes to user accounts and system permissions
 - ❖ Using the data search or creating reports
 - ❖ Accessing patient data

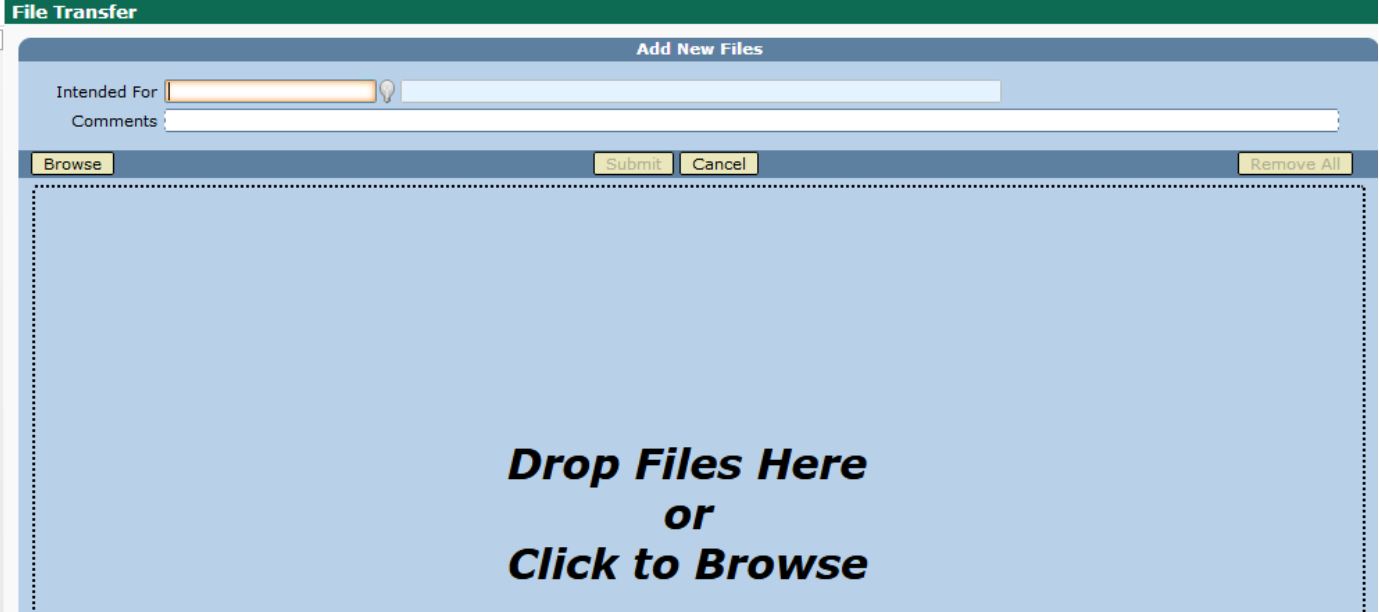
New Features to Protect Data:

SEER*DMS File Transfer Module

A secure File Transfer mechanism was built into SEER*DMS. This increases data security by reducing the exposure of data to external systems.

This system can be used by:

- ❖ Registry users with SEER*DMS accounts
- ❖ IMS staff with SEER*DMS accounts
- ❖ Limited access users – facility staff can be given a limited access account. These users can only access data files that they transfer; and data files that are transferred to their account.



The screenshot displays the 'File Transfer' interface. At the top, there is a green header with the text 'File Transfer'. Below this is a sub-header 'Add New Files'. The form contains two input fields: 'Intended For' and 'Comments'. The 'Intended For' field has a light blue background and a lightbulb icon. Below the input fields are four buttons: 'Browse', 'Submit', 'Cancel', and 'Remove All'. The main area of the form is a large light blue rectangle with a dotted border, containing the text 'Drop Files Here or Click to Browse' in bold black font.


New Features to Protect Data:

Imports from Trusted Partners

A feature was added to allow a trusted individual from a facility to submit import files. For example, for a trusted individual at a hospital to upload a file of abstracts.

This was added to reduce the need for access to registry systems for the purpose of loading data files. This feature was included in penetration testing to ensure that the user has no access to other parts of the system.

The user can only see files that they uploaded. They cannot access any other data. Any file that they upload is stopped in an Import Review so that the data can be validated by registry staff before entering the workflow.

Import		(1) 
<input checked="" type="checkbox"/>	Permission	Description
<input checked="" type="checkbox"/>	import_electronic_limited	This permission allows a user to upload files to the import manager. The user can see files that they uploaded. They cannot view any other files. They cannot delete files that they uploaded. Any file that they upload will stop in Import Review.