**Simple Dose Audit #21170**

**SVP’s: Raymond Auger**

**SME’s: Bill Mullins, Gaurav Sachdeva, Padma Ajit**

**POC: Jeanne Willis**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Project Name** | **Project Type** | **Oversight** | **Lead** | **Sub-Lead** | **Staff** |
| 21170 - SimpleDose | Audit | Sarah Kubiak | Michael Bavasso | Seun Mafi | Dan Benner, Daniel Rodrigues, Ashish Joshi |

**Brainstorming**

* User Access = Michael, Dan, Daniel
  + Review of System Design Document
  + Critical File Access / Privileged Access / User Recertification
    - Not looking at Frontend (or endpoint)
    - Sarah will provide examples from a prior audit \*\*
* Where are these data points or storage located and who has access?
* Where are the key execution files? Libraries, directories…
  + User Provisioning Method (focus on back end process)
  + Is this Oracle with UNIX servers… Who has Root access? (Phil Albert?)
  + SimpleDose Operating System
    - If there is Root, does it get logged or audited?
  + Not testing the provision process, only who is making the reviews.
    - Is the enterprise provisioning process being used?
    - What tool is being used for access requests?
  + How is Periodic Access Review (PAR) performed and who reviews the access for the critical program data files specific to SimpleDose?
    - Critical files and directories
    - Full directory names and file
  + What is the Deprovisioning process for critical files, libraries, and directories?
    - What are the critical systems files for SimpleDose?
    - Which users and groups have access to these critical system files?
      * Program files that allow SimpleDose to function
      * List of users and groups
      * Associated permissions
    - If there are any new directories being pushed into production in the future, is there a validation process that permissions are accurate from pre-production into production.
    - What is the user provisioning process for these critical system files?
    - Is there a revalidation process?
    - How are these critical system files restricted?
    - What is the security over these CLDs?

After walk-thru…, obtain a system generated list of users with access to the SimpleDose application by applicable folders, servers, libraries, directories, or storage areas being used by SimpleDose.

Include user name, ID, access date, user role or job function

Obtain names of folders, servers, libraries, directories, or storage areas being used by SimpleDose.

RCA / Testing = Perform testing to ensure the following:

1. Access is appropriate based on individual’s job responsibility.
2. Determine if accounts are still applicable to SimpleDose.