# Access Control and Password Security Management in Pharmaceutical Industry

**Akhila Gandraju[1], Vishnu Vardh R[2], Pyda Venkata Harsha Vardhan[3], Maged Mohammed Abdo Mohsen[4], Praveen Halagali[5], Girish M S[6], Hemanth Kumar S[1*]**

[1,1*] Department of Pharmaceutics, Pharmaceutical Quality Assurance Group, JSS College of Pharmacy, Mysuru, JSS Academy of Higher Education and Research, Mysore, Karnataka-570015
[2,3,5]Department Of Pharmaceutics, JSS College of Pharmacy, JSS Academy Of Higher Education And Research (JSSAHER), Mysuru-570015, Karnataka, India.

[4]Ph.D Scholar Department of Pharmaceutics, JSS College of Pharmacy, JSS Academy Of Higher Education And Research (JSSAHER), Mysuru-570015, Karnataka, India.
[6]Department of Pediatric and Preventive Dentistry, JSS Dental College & Hospital, JSS Academy of Higher Education and Research, Sri Shivarathreeshwara Nagar, Mysuru-570015, Karnataka, India

**[*] Correspondence for author**

**Hemanth Kumar S**

Department of Pharmaceutics, Pharmaceutical Quality Assurance Group, JSS College of Pharmacy, JSS Academy of Higher Education and Research, Mysuru-570015, Karnataka, India
Email Id: hemanthkumar@jssuni.edu.in

**Abstract**

Access Control and Password Security Management plays a vital role in most of the pharmaceutical industry. It is a critical requirement of electronic record compliance, as described in the Food and Drug Administration (FDA) 21 CFR part 11.10 (a) and European Medicines Agency (EMA) Annex 11, section 4. Due to increasing scrutiny and inspection from the FDA and other regulatory bodies as well as need comply with the industry standards such as Good Manufacturing Practices (GMP), Good Distribution Practice Standards (GDP), Good Storage Practices (GSP) and other relevant standards set by the WHO. Therefore, pharmaceutical industry needs to implement and enforce consistent security practices. The purpose of access control and password management is to define minimum computer security requirements to protect application data and resources with respect to confidentially, integrity and availability for computerized systems. To lay down a procedure for access control and password security management of the equipment/instrument/system facilitated with password control. This is relevant to all the systems, software's, programmable logic controllers and other electronic devices used in the pharmaceutical industry.

**Keywords:** Good Manufacturing practices, Good Distribution Practice Standards, Good Storage Practices, Software's, Computers, Programmable Logic Controllers and Device

## INTRODUCTION:

Access Control and Password Management is an integral part of 21 CFR Part 11 i.e., Identity Management and Identity Access Governance helps companies to stay in control of an employee lifecycle and to audit it Access Requests will be compliant to company's policies and regulations processed and automatically provisioned[1-3]. It describes Information about how account information is managed, who is authorized to access resources, which system is authoritative for individual attribute information and what information can be input into attributes and also provides an Enhanced operational efficiency, increased security and flexibility to meet organization's unique requirements. On a regular basis industry reports proof that missing control of identities lead to data loss or other damages to an organization. These issues pop up usually due to missing segregation of duties and revocation of access rights[4,5].

- **The Computerized System Validation:** Is defined as a documented activity of certifying that a computerized system does absolutely or precisely what it is planned to perform in a harmonious and reproducible manner.
- **Access levels:** This is a security feature that limits access to the system based on the defined set of permissions.
- **Computerized Systems:** Information technology hardware, software and network components, together with controlled functions and associated documentation, which are used to perform business functions.
- **System:** System shall consist of equipment/instrument/system.
- **GxP:** International pharmaceutical requirements and applicable national legislation and include GMP, GLP, GDP, good pharmacovigilance practice and medical device regulation.

Access Control and Password Security Management is an Essential part of the pharmaceutical industry mainly focuses on **[12]**:

- Management of the users, credentials, policies, and access within your system.
- Synchronizing identities between directories, databases and applications.
- Self-service password, group, and certificate management.
- Increase of admin security with policies, privileged access and roles

It gives a clear idea of Observed rules relating to the segregation of duties.

## REGULATORY VIEWS ON COMPUTERIZED SYSTEM VALIDATION:

1. Validation of Computerized Systems- Core Document PA/PH/OMCL (08) 69 R7 **[6,7]**: Defines the basic Principle of computerized system validation used within the official medicines control laboratories (OMCLs) & its impact on the quality of results, document control and data storage.
2. . International Conference of Harmonization (ICH) Q7 (R2), GMP **[8]**: Related computerized system should be validated.
3. Appendix 5 Validation of Computerized Systems **[9]**: Computerized systems should be maintained in the validated state with risk-based controls appropriate to the different stages of the system life cycle.
4. International Organization for Standardization (ISO) 13485; Clause 7.5.2.1**[10]**: validation of the application of

computer software for service provision shall conform to specified requirements. \

5. Organization for Economic Co-Operation and Development (OECD) No.1 GLP [11]: Ensures that computerized systems used in the study have been validated.

6. European Union (EU) GMP Annex 11[12]: Computerized Systems: States that system application should be validated; IT infrastructure should be qualified.

Most common computerized system that needs to be validated frequently in pharma industry is as follows [13]:

- Environmental Monitoring System (EMS)
- Automated manufacturing equipment [(Programmable Logic Controller (PLC) / Distributed Control System (DCS)/Supervisory Control and Data Acquisition (SCADA)]
- Line Automation (PLC / DCS/ SCADA)
- Building Management System (BMS)
- Document Management Systems
- Laboratory Management Systems
- Process Automation Systems (PLC/ DCS/ SCADA)

**CHALLENGES OF PASSWORD MANAGEMENT [4] [14]:**

- With increase in usage of systems, there is also increase in the number of passwords we have to remember and manage.
- Passwords used for the Different Systems / Equipment's causes Dilemma.
- Some of the passwords are common
- On the other side, when the different password is used for different equipment's user may have the chances to remember easy or weak passwords or even write down them; which is again harm to the security of the systems concerned.
- Passwords are not revised or changed frequently.
- Exchanging of private User-Identification.

**PROCEDURE:**

**MANAGING ACCESS LEVEL AUTHORIZATION [3]:** Is a broad term that encompasses the use of different Instruments / Equipment's to identify, authenticate, and authorize users through automated means. Flow of access control system is depicted in **Figure 1**

The goal of managing access level authorization is to simplify the supervision of these tasks

- At the time of qualification of new equipment or as per the notification of quality management systems, the process owner/system owner has to refer the user manual of the new equipment and prepare the access control and password management record, based on the requirement, support from the vendor or Site/ plant IT will be taken.
- Access control and password management record template can be modified as per the number and nomenclature of access levels for the respective systems.
- Approved record shall be maintained securely with site Quality Assurance department, in case of common user id where password management log is in use, password shall be handwritten on the approved management record (Use the updated/latest version of record for recording the password).
- Access privileges are granted at the software level, one or more than one

equipment may be connected to the software.

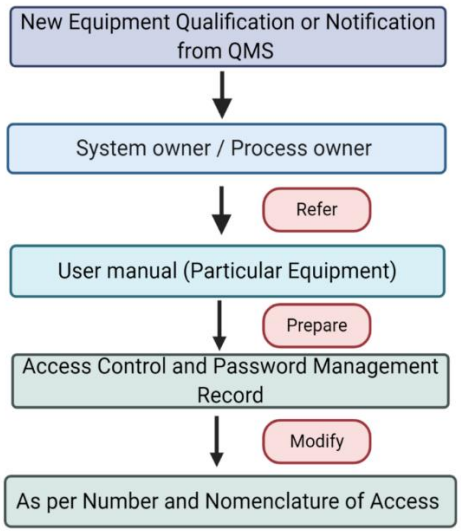


**Figure 1: Flow of access control system**

**Examples of Nomenclature of Access Le vel**

LEVEL 1 – Operator / Analyst

LEVEL 2 - Supervisor or Executive

LEVEL 3 – Manager or Administrator

LEVEL 4 – External Service Provider or Vendor / System Owner / User

**MANAGING COMMON USER ACCESS CREDENTIAL [15]:**

For systems where, unique ID is not supported, Management of Common user access credentials is explained in **Figure 2**

- Site QA or Plant QA person managing user access will be responsible for printing of the access request form booklets.
- The booklet form mainly consists of serial numbers.
- User who ever needs to have the access must complete the required training for the system & submit the completed Access Request Form to System Owner for authorization.
- System Owner/Process Owner/Designee will review the training records & authorize the access request form.
- User/System Owner will submit the completed Access Request Form for Quality Assurance personnel approval.
- Site QA head/Designee will approve or reject the request. Reason for rejection has to be assigned and captured on the request form. If the request is rejected then the person/ user has to undergo the training once again.
- User/System Owner will submit the approved form to the designated administrator. Administrator will verify the access request form for completeness, grant the access, update the request form and file the completed form for ready reference.
- Administrator will provide the access credential for the requested access level directly to the user after verification. Note: For the operator level , access shall be assigned by the department head, since operator level user will only have permission to start or stop the operation
- Administrator will maintain the list of active users for every system and shall review and update the active user list on a yearly basis/during periodic review or as needed as per - List of Active Users.

- Administrator will reset the password for the system upon request, in case of the following events,

➢ Password revealed for demonstration or training.

➢ Temporary access in case of emergency.

➢ At the time of re-qualification.

➢ As part of recommendation of QMS documentation.

- Upon resetting the password of any system, administrator will update the section “Password Management Log” of
- Administrator will identify and inform the respective users for the changed password
- Administrator will ensure the periodic revision of the password for all access levels in line with company password security policy, subject to system capability.
- Users are not authorized to change the password of common user access credentials.
- Where common password cannot be changed, the de-activation form is not required. Where password can be changed, deactivation form will be filled & submitted to QA for maintaining the list of authorized users.

**Note:** In case of external vendor/supplier access request shall be provided with the applicable details.

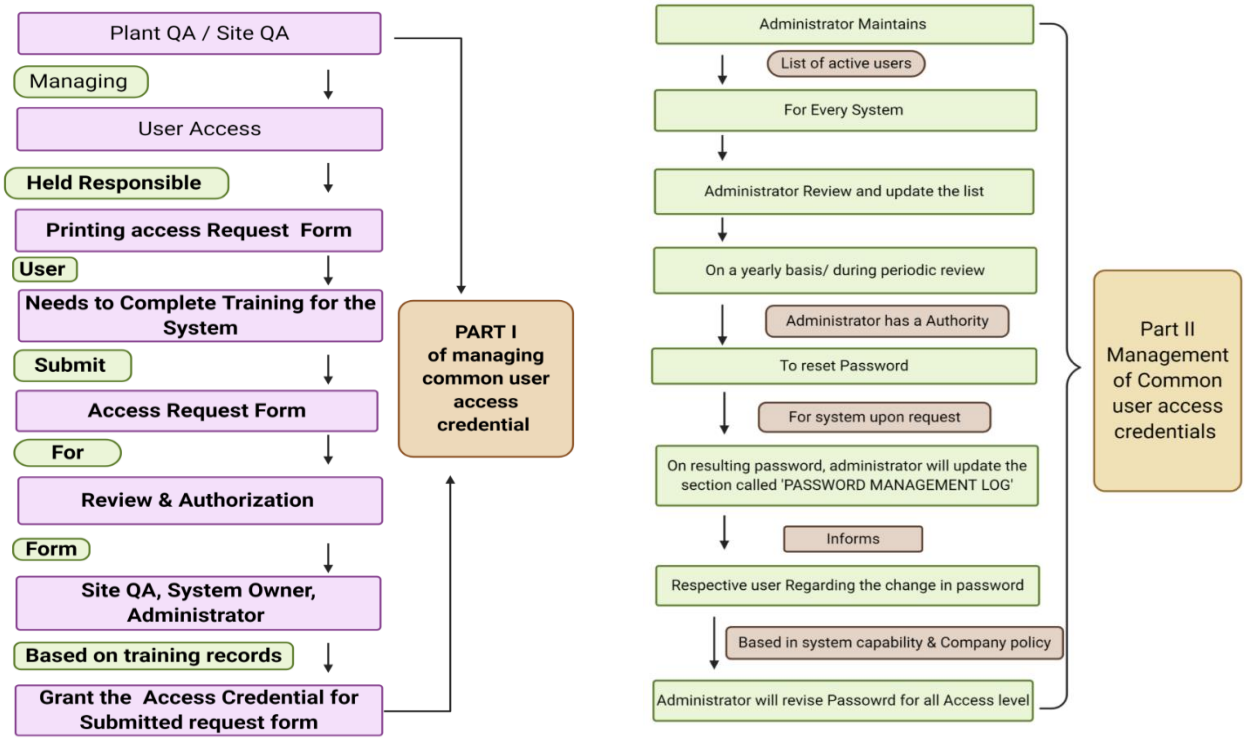


**Figure 2: Management of Common user access credentials**

**MANAGING INDIVIDUAL USER ACCESS [3] [16]:**

Access request form is given in **Figure 3**

- Site QA person managing user access will be responsible for printing of the Access Request Form booklets.
- User must complete the required training for the system & submit the completed Access Request Form to System Owner for authorization.
- completed Access Request Form for QA approval.
- System Owner/Process Owner/Designee will review the training records & authorize the access request form.
- User/System Owner will submit the Site QA head/Designee will approve or reject the request. Reason for rejection has to assigned and captured on the request form.

- User/System Owner will submit the approved form to the designated administrator.
- Administrator will verify the access request form for completeness, grant the access, update the request form and file the completed form for ready reference.
- Administrator will provide the access credentials directly to the user, after verification.
- Administrator will maintain the list of active user for every system and shall review and update the active user list on a yearly basis/during periodic review or as needed - List of Active Users.
- User has the responsibility to change/reset the password upon receiving the password for the first time and every time the password has been reset by administrator

## MODIFICATION/DEACTIVATION OF USER ACCESS:

- Department head/Designee/User will initiate the request & will submit the completed Access Request Form to System Owner/Process Owner for authorization.
- Site QA head/Designee will approve or reject the request. Reason for rejection has to assigned and captured on the request form.
- User/System Owner will submit the approved form to the designated administrator.
- Administrator will verify the access request form for completeness, modify/deactivate access, update the request form and file the completed form for ready reference.
- User modification/deactivation must be completed within Specified calendar days, from the day access is no longer required.

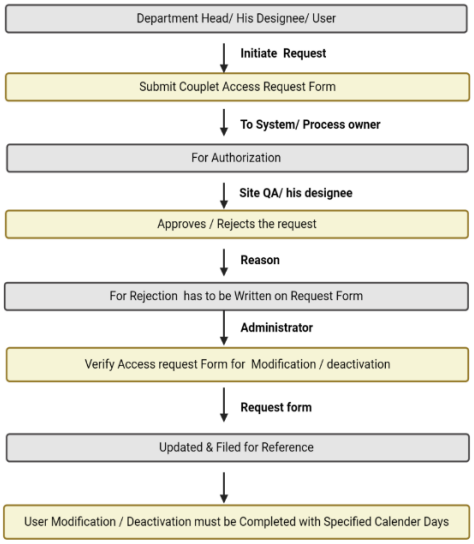


**Figure 3: Access Request Form**

## PERIODIC USER ACCESS REVIEW

Flow of periodic user access review is given in **Figure 4.**

- User access review must be performed for a system at least once per year or as per the Company's Norms.
- Periodic user access review schedule shall be prepared in the Starting month of every year to distribute the work load evenly throughout the year by QA team.
- While preparing the schedule last review date should be considered.
- First schedule of the year should be called as an Original & then after any new equipment's/instruments/systems shall be included by preparing the addendum i.e addendum I, II, III etc. At the time, next year during preparation of schedule all addendum shall be merged in original schedule.
- Administrator will perform the periodic user access review using the checklist. User Access Review Checklist) as per the schedule.
- Review must be completed within time limits from the planned schedule

- The process owner/system owner has to confirm that the user access to the system is as per this SOP.
- Periodic user access review checklist shall be approved by site QA after the closure of all identified gaps and the record is maintained with the QA department for ready reference.
- Administrator will update the schedule with the actual completion date for tracking.
- Site QA will perform the monthly review of the schedule & sign.
- At end of the year, the completed schedule will be submitted to the site QA
- QA will verify the schedule for completeness & file it for ready reference.

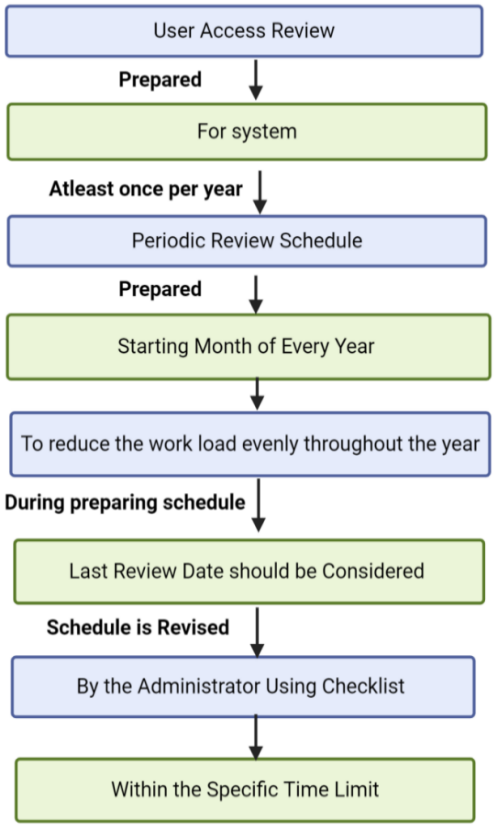


**Figure 4: Flow of periodic user access review.**

**PASSWORD SECURITY [12]:**

- User access to the company network, applications or data requires appropriate authorization.
- System and application permitting, new user accounts force the user to select a new password upon initial access.
- System and application permitting, a minimum character is required for a password.
- System and application permitting, user accounts are forced to create a new password every now and then.
- System and application permitting, account access must be locked after a maximum unsuccessful login attempts for a minimum time period.
- System and application permitting, the reuse of the last passwords must not be allowed.
- System and application permitting, the use of a username or User ID as a password must not be allowed.
- Default passwords must be changed prior to production use.
- System and application permitting, authentication and credentials must be encrypted at rest and in transit, given the level of sensitivity, value and criticality that the data has to the company.
- System and application permitting, system level accounts must be tied to individual users.

**Example of template**
**Access Control and Password Management Record:**

| | | | | |
|---|---|---|---|---|
| Equipment Name | | Software Name | | |
| Equipment Number* | | Equipment Location/ Place | | |
| Frame Work / Parameter | [Access level-1] | [Access level-2] | [Access level-3] | [Access level-4] |

**Password Management Log:**

| Reset Date | Access Level -1 | | Access Level-2 | | Access Level-3 | | Access Level-4 | |
|---|---|---|---|---|---|---|---|---|
| | User ID | Password | User ID | Password | User ID | Password | User ID | Password |

**Example of Access Request Form:**

| | | | |
|---|---|---|---|
| Purpose for Request (Tick as applicable) | □ Creation | □ Modification | □ Deactivation |
| a) First Name | | b) Last Name | |
| c) Equipment/Instrument Name | | d) Software Name | |
| e) Access Level | | f) Department | |
| g) Requested by User | Signature with Date: | | |
| h) Authorized by (System owner / Process Owner) | Signature with Date: | | |
| i) Comments (If necessary) | | | |
| j) Approval (Quality Assurance Personnel) | □Approval □Rejection Signature with Date | Reason for Rejection | |

**Example of a list of active users:**

| Equipment / Instrument Name | | | | |
|---|---|---|---|---|
| Software Name | | | | |
| Sr.No. | User ID | User Name | Access Level | Comments (if any) |
| 1 | | | | |

**Example of checklist for user access review:**

| Equipment Name | | |
|---|---|---|
| Software Name | | |
| Review Period or Frequency | | |
| Sr.No. | Review Period Check Points | Observations / Comments |
| 1 | Make the list of the available users in the systems | |
| 2 | Check for the availability of the 1.0 for the system/ equipment | |
| 3 | Check the access level assigned for the system | |
| 4 | Ensure approved request from is available for the users | |

**CONCLUSION:**

The application of access control becomes a key instrument for developing layers of security for protecting the assets of a pharmaceutical corporation within each of its facilities. It describes Information about how account information is managed, who is authorized to access resources, which system is authoritative for individual attribute information, and what information can be input into attributes and also provides enhanced operational efficiency, increased security, and flexibility to meet the organization's unique requirements. This type of management reduces operational risk and protects critical data from unauthorized access. By doing this it concludes meeting the requirements of audits.

**REFERENCES:**

1. Computer System Validation, Prepared by 21 CFR Part 11(FDA), http://www.computersystemvalidation.com/component/content/article.html?id=48:what

2. Security solutions to protect facilities, Prepared by Johnson Controls, https://www.tycois.com/solutions-by-industry/enterprise/pharmaceutical

3. SOP on Password Policy for computers and software's in pharmaceutical plant, Prepared by Sachin Choudhary, http://pharmapathway.com/sop-on-password-policy-for-computers-and-softwares-in-pharmaceutical-plant/

4. Password Management, Prepared by Government of the Hong Kong Special Administrative Region, https://www.infosec.gov.hk/english/technical/files/password.pdf

5. Identity & Access Management, Prepared by Patecco dynamic identity systems, https://patecco.com/en/?page_id=25

6. 12. E. Bertino and K. Takahashi, Identity Management: Concepts, Technologies and Systems, Artech House, 2011, p. 198.

7. PA/PH/OMCL (08) 69 R7, Prepared by General European OMCL Network (GEON) Quality Management Document, https://www.edqm.eu/sites/default/files/guidelines-omcl-computerised_systems-core_document-march2018.pdf

8. ICH Q7 (R2), Prepared by ICH Harmon ized Tripartite Guideline,

https://www.ich.org/fileadmin/Public_We b_Site/ICH_Products/Guidelines/ Quality/Q7/Step4/Q7_Guideline.pdf

9. ICH Q7 (R2), Prepared by ICH Harmonized Tripartite Guideline,

https://www.ich.org/fileadmin/Public_We b_Site/ICH_Products/Guidelines/ Quality/Q7/Step4/Q7_Guideline.pdf

10. ISO 13485; Clause 7.5.2.1, prepared by International Organization for standardization, http://sic.com.ua/wp-content/uploads/2009/11/iso-13485-2003.pdf

11. OECD Principles of good Laboratory Practice, Prepared by organization for economic Co-operation and development (OECD),

https://ntp.niehs.nih.gov/iccvam/suppdocs/ feddocs/oecd/oecd_glpcm.pdf

12. Annex 11: Computerized Systems, Prepared by European Commission, http://academy.gmp-compliance.org/guidemgr/files/ANNEX11 _01- 2011_EN.PDF

13. Computerized System Validation, ivyworks, http://ivyworks.net/compliance_csv .html

14. Privileged Account Management, Prepared By ARCON, https://arconnet.com/case-studies/ARCOS_Pharma_Industry.pdf

15. Case Study on Identity and Access Management in Pharmaceutical industry, Prepared by Aalto University, https://pdfs.semanticscholar.org/b8b2/ae63 633e83e9c5d71f38d2e2b02c793a2b26.pdf

16. SOP for Access Control System, Numbering and Usage, Prepared by Sachin Choudhary, http://pharmapathway.com/sop-for-access-control-system-numbering-and-usage/.