UC IRVINE | INTERNAL AUDIT SERVICES

Medical Center Lockbox Access

Internal Audit Report No. I2023-202

December 19, 2022

Prepared By
Darlene Nuñez, Senior Auditor
Reviewed By
Niran Joshi, Associate Director
Approved By
Mike Bathke, Director

UCI Internal Audit Services

December 19, 2022

CRYSTAL DEXTER
DIRECTOR
PATIENT FINANCIAL SERVICES

APRIL MONTES
DIRECTOR
PROFESSIONAL BILLING GROUP

RE: Medical Center Lockbox Access Audit
Report No. I2023-202

Internal Audit Services has completed the review of the Medical Center lockbox access and the final report is attached.

We extend our gratitude and appreciation to all personnel with whom we had contact while conducting our review. If you have any questions or require additional assistance, please do not hesitate to contact me.

Sincerely,

Mike Bathke
Director

Attachment

C: Audit Committee

I. MANAGEMENT SUMMARY

In accordance with the fiscal year (FY) 2022-2023 audit plan, Internal Audit Services (IAS) conducted a review of Medical Center Lockbox Access. In general, controls and processes appear to be functioning as intended. Based on the audit work performed, some internal controls need improvement and should be strengthened to minimize risks, ensure compliance with University policies and procedures, and/or best business practices. Specifically, IAS notes the following concerns.

Sharing Usernames and Passwords – Professional Billing Group (PBG) staff shared usernames and passwords to access the lockbox portal which is prohibited by University policy. This observation is discussed in section V.1.

Review of Lockbox Access – PBG and Patient Financial Services (PFS) did not regularly review and document user access to the PNC Bank lockbox portal. Four PBG users who have separated from the University or are no longer with the department continue to have access to the lockbox portal. In addition, some PBG and PFS users have not accessed the portal between seven to 32 months and continue to have access. Furthermore, the PFS administrator who is granting user access is also performing the periodic user access review which is an inadequate separation of duties. This is discussed in section V.2.

II. BACKGROUND

PBG is a department under the UCI School of Medicine (SOM) that serves as UCI's in-house physician billing unit who process and handle all professional fee billing to insurance companies. PBG services approximately 900 UCI physicians and 30 departments. PBG has their own finance team that is responsible for accessing and identifying all electronic fund transfers and check payments to ensure they are properly posted. The PBG finance team employs approximately 18 full time staff, including a Finance Manager who reports to the Director.

PFS is a unit under UCI Health that serves the hospital and clinics by processing and handling all patient fee billing and collections. The posting unit is responsible for posting payments received. Payments are received through various channels including the Medical Center's post office box and lockboxes. There are approximately 30 full time staff in the posting unit who report to a supervisor.

PBG and PFS have established lockboxes with PNC Bank to simplify and streamline accounts receivable administration. Electronic and check payments and correspondence are routed into PNC accounts to help provide efficient reporting, timely cash application, and information management. PNC Bank provides same day access to check images and other remittance information. PBG and PFS have view/read only access to payments and correspondence through an online portal. PBG and PFS manage user access to the PNC lockbox portal independently.

III. PURPOSE, SCOPE AND OBJECTIVES

The purpose of this audit was to perform a review of Medical Center lockbox access to assess business risk, internal controls, and compliance with University policies and procedures. The scope included reviewing and the sample testing of data from January 1, 2022 through October 30, 2022.

The audit included the following objectives:

1. Obtain an understanding of how user access is granted and verify that access is properly requested, approved, and that proper separation of duties exists;

2. Determine if user access and permissions are periodically reviewed and documented to ensure that only authorized individuals have access;

3. Evaluate the type of information outside vendors are accessing and the level of access provided. If protected health information (PHI) is accessed, verify that a Business Associates Agreement Appendix exists in accordance with UC policy; and

4. Review the training provided to lockbox users and determine if it is adequate to ensure data is protected and secured.

IV. CONCLUSION

In general, controls and processes appear to be functioning as intended. However, PBG and PFS could improve controls and processes by prohibiting the sharing of usernames and passwords, reviewing user lockbox access, and establishing a process for deactivating dormant users.

IAS discussed observation details and recommendations with management, who formulated action plans to address the issues. These details are presented below.

V. OBSERVATIONS AND MANAGEMENT ACTION PLANS

1. Sharing User Names and Passwords

Background

UCI Policy *Sec. 714-17: Using University Administrative Information Systems* states that maintaining the confidentiality of passwords is critical in preventing misuse, intrusion, and theft. Each user is personally responsible for the use of their logon identification and password. They are not to share their confidential password

with anyone, including supervisors, co-workers, family members, or friends. Additionally, UCI's *Computer and Network Use Policy* states: "To help protect computer and network resources files, users are responsible for setting passwords appropriately, and for keeping passwords confidential by not giving them to another person, and for following the other appropriate security procedures."[1]

Observation

In discussion with PBG's Finance Manager, IAS found that usernames and passwords are shared amongst staff when items are pending and those staff are unable to get the correct access into the PNC lockbox portal. IAS advised management to immediately refrain from sharing usernames and passwords as this is prohibited by University policy.

Management should review all PNC lockbox users and ensure that each authorized user has their own unique username and password to distinguish that user from other users and to provide accountability.

Management Action Plan

As of November 1, 2022, usernames and passwords are no longer shared amongst staff and all users have been assigned a unique username and password. Management no longer allows the sharing of usernames and passwords. This was communicated to staff on several occasions verbally and in email on December 7, 2022.

Due date: Completed during the audit

2. Review of User Lockbox Access

Background

Per *UCI Information Security Standard (ISS) 9.2 General Account Management*, units must review accounts and access rights at least annually and remove access that is no longer needed. Also, accounts that have not been accessed for 180 consecutive days (six months) must be reviewed and deactivated if no longer needed.

Observation

PBG

PBG's lockbox access is not periodically reviewed and documented to ensure it is appropriate in accordance with UCI ISS 9.2. IAS reviewed the user listing and found:

[1] *Sec. 714-18: Computer and Network Use Policy*, UCI Administrative Policies & Procedures, Sept. 2011, https://www.policies.uci.edu/policies/pols/714-18.php.

- Four users who were no longer employed by the University or PBG still had active accounts.
- Six PBG users who have not accessed the system between seven to 32 months are still enabled users.

Failing to perform user access reviews on a regular basis results in a higher risk for a terminated employee to inappropriately access the lockbox and PHI.

All PBG lockbox user accounts should be reviewed to verify the level of access, to disable access for those who no longer need access, and to deactivate dormant accounts. This will prevent vulnerabilities that may arise from situations due to account privileges and access to resources.

Since deleting or removing access would also delete the logs, user accounts should be deleted after the four-year retention period has passed in accordance with the UC Records Retention schedule. Periodic reviews should be documented and reflected in internal policies and procedures.

PFS

PFS stated they perform periodic user access reviews. However, seven PFS users who have not accessed the system between seven to 13 months still have active accounts. Also, the access review is not documented and therefore there is no evidence of the review. Finally, the person approving and granting access is also performing the user account reviews, which is an inadequate separation of duties. To minimize the occurrence of both erroneous and inappropriate actions, responsibilities should be separated and no one employee should have complete control.

PFS should develop a process to disable accounts for dormant users and access should be deleted or removed after the four-year retention period has passed in accordance with the UC Records Retention Schedule. The established process should be documented and included in their written internal policies and procedures.

Management Action Plan

PBG

Management will conduct a review of all user accounts including the level of access and will disable access for dormant users and for those who no longer need access. Management will also develop a formalized user access review policy and procedure to include:

- Establishing a consistent review schedule;
- Identifying roles and access permissions;

- Establishing a process to disable and delete access for dormant users after a period of time;
- Establishing a record and ongoing document of all changes made to accounts, including when to disable and delete access;
- Establishing a regular check on an employee's current permissions to ensure they are appropriate; and
- Establishing who is responsible for the review.

Due date: March 1, 2023

PFS

PFS will also develop a formalized user access review policy and procedure to include:

- Establishing a consistent review schedule;
- Identifying roles and access permissions;
- Establishing a process to disable and delete access for dormant users after a period of time;
- Establishing a record and ongoing document of all changes made to accounts, including when to disable and delete access;
- Establishing a regular check on an employee's current permissions to ensure they are appropriate; and
- Establishing who is responsible for the review, which will be performed by the supervisor and reviewed by the Assistant Director to ensure proper separation of duties.

Due date: March 1, 2023