Public Health Services
Audit of Information Technology
Maricopa County Internal Audit
July 2020

Why This Audit Is Important

Public Health Services (PHS) provides community health, disease control, and clinical services programs to protect and promote the health and well-being of all Maricopa County residents. PHS utilizes several software applications to support its mission. It is important to protect confidential medical information and records contained in certain applications.

We performed this audit to assess whether PHS has established adequate controls: 1) for granting and monitoring access to key electronic health record software applications, and 2) to ensure that terminated network user accounts are removed in a timely manner.

Key Findings

- Written procedures are needed to help manage user access appropriately and consistently.
- Reviews of user access rights should be performed periodically.
- Procedures can be improved to ensure timely termination of network user access.

All key findings requiring corrective action were addressed through agreed-upon management action plans.

What We Audited

Below is a summary of work performed and findings. Corresponding recommendations and responses start on page 3. The responses were approved by Marcy Flanagan, PHS Executive Director, on June 2, 2020. More detailed observations and recommendations were communicated to management throughout the audit process.

Accessing Key Applications

Background – Using secure network connections to restrict access to an application can protect the application, and its data, from unauthorized users or intruder attacks.

Observations – We interviewed key employees, reviewed documentation, and observed system accessibility for key health record software applications. We found that some weaknesses existed. Detailed technical findings and recommendations were communicated directly to PHS and corrective action plans are in place. For security purposes, further details are restricted from this public report.

User Access Procedures

Background – User access management is a process of controlling who is authorized to access a computer system and what they can access within the system. User access policies and procedures provide clear and consistent guidance to help ensure appropriate practices are followed for managing access requests and changes.

Observations – We interviewed key employees and reviewed user access management practices and learned there were no written procedures for managing user access to the electronic health record applications (**Recommendation 1**).

Written procedures are needed to help manage user access appropriately and consistently.

User Access Reviews

Background – Periodic reviews of user access rights can help ensure that the level of access allowed for each application user is appropriate and restricted to functions required by a user's current job responsibilities.

Observations – We interviewed key employees and found that user access reviews were not performed and documented for key electronic health record applications or for network accounts. In addition, there were no written procedures for conducting user access reviews (**Recommendation 2**).

Terminated Employee Network Access

Background – Access to the network, where key applications are saved, is an important security consideration. Prompt removal of network user access when a user's employment is terminated helps ensure key applications and data cannot be accessed without authorization.

Timely termination of network user access can be improved.

Observations – We conducted interviews, reviewed documentation, and performed testing on a sample of network users to determine if users had access removed within 24 hours of termination, as required by County policy. We found that access for some terminated users was not removed in a timely manner, but we determined they did not access their accounts after termination. There was no consistent procedure in place for ensuring that OET was notified of terminations for purposes of removing network access (**Recommendation 3**).

Additional Information

This audit was approved by the County Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing. This report is intended primarily for the County Board of Supervisors, County leadership, and other County stakeholders. However, this report is a public record and its distribution is not limited. If you have any questions about this report, please contact Mike McGee, County Auditor, at 602-506-1585.

Recommendations and Responses

Recommendations	Responses
1 Establish written user access procedures in accordance with County policy.	Concur – in progress Department will work with clinic management to develop policy and procedures to address this. Target Date: 08/31/2020
2 Implement policies and procedures for conducting user access reviews of key electronic health record applications and Active Directory accounts at least annually.	Concur – in progress Department will work with clinic management to develop policy and procedures to address this. Target Date: 08/31/2020
3 Establish written procedures to ensure that OET is notified of terminated users to ensure network access is removed within 24 hours of departure date, in accordance with policy.	Concur – in progress Department will work with clinic management, HR, and OET to develop policy and procedures to address this. Target Date: 08/31/2020