Fairfax County Internal Audit Office

Fairfax- Falls Church Community Services Board
Data Classification Audit
Final Report

February 2018

"promoting efficient & effective local government"

Background Information

General

Agencies within Fairfax County Government are responsible for handling sensitive and confidential information during the normal course of operations. County agencies are required to determine data classifications for information processed in County information systems, based on County, legal, and regulatory requirements. Data classifications are used to determine the nature and extent of security and system controls that must be implemented to protect data in information systems. The County Department of Information Technology (DIT) Information Technology Security Policy 70-05.01 defines four pre-determined classes of data. The four classes are confidential, sensitive, internal use and public use. Confidential or sensitive information stored in County information systems includes data such as client or patient health and Social Security Number (SSN), social services and domestic violence information. Several county agencies are required to comply with Health Insurance Portability and Accountability Act (HIPAA) and Virginia codes 63.2-104 and 63.2-104.1 for protection and security of social services and domestic violence information.

Executive Summary

Our audit focused on determining whether policies and procedures were established for classifying agency's data based on the level of sensitivity. Additionally, we focused on determining whether agencies handling sensitive information have controls in place to protect confidential records. Finally, we reviewed access to information to ensure it was based on a business need with least privileges access rights. Our audit population included three county agencies. A report is being issued for each agency audited.

Fairfax- Falls Church Community Services Board (CSB) uses various systems to store and manage client electronic mental health services information and financial records. We noted that the CSB data was identified and classified in accordance with the County Information Security policy and external regulations, user access rights were assigned based on their job responsibilities, disclosure of data was properly authorized and complied with County policies and external regulations. However, we noted the following exception where compliance and controls could be strengthened:

We found the CREDIBLE system access for one user, out of the twenty tested, was not revoked or changed after the individual transferred to another County agency. CSB did not have formal procedures requiring the periodic review of system users.

Scope and Objectives

This audit was performed as part of our fiscal year 2016 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered the period of July 1, 2016, through June 30, 2017. The objectives of the audit were to determine that:

- Information systems have been identified and classified in accordance with Information Security Policy 70-05-01 and external regulations.
- There were proper controls over access and changes to confidential and sensitive data.
- Disclosure of sensitive and confidential data was proper and authorized

Methodology

Our audit approach included review of Information Technology Security Policy 70-05.01, to gain an understanding of data classification determination methodology. We reviewed HIPPA regulations to gain understanding of the security rules for information systems processing HIPAA protected health information (PHI). We interviewed department management and staff responsible for data classification policies and procedures, system user access, practices for the disclosure, and protection of sensitive or confidential data. We obtained a list of the systems from CSB and determined the reasonableness of data type classification.

We selected one of four CSB information systems for testing. CREDIBLE, the primary CSB information system used for storage of confidential and sensitive information, was selected for testing. We conducted a system walk-through to gain an understanding of the data stored in this system. We performed user access rights test for this system to ensure user rights are assigned based on their job responsibilities. Lastly, we reviewed disclosure of confidential information or sensitive information for authorization and security.

The Fairfax County Internal Audit Office (IAO) is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the County Executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the County Executive and the Board of Supervisors, and IAO reports are available to the public.

Findings, Recommendations, and Management Response

Periodic Review of System User Access

We found that the CSB did not have formal procedures requiring the periodic review of system users to validate the system access by staff. We found one CREDIBLE system user, out of twenty active user accounts tested, for which access was not terminated or modified after the individual transferred to another county agency.

CSB is required to comply with DIT Security Policy 70-05 01 for system user account administration. DIT Security Policy 70-05 01 Section 3.5.2 *Account Administration* states:

> User access to Fairfax County systems shall be periodically reviewed and adjusted as necessary by the system owners to ensure that access is in accordance with the concept of least privilege. Agency Information Security Coordinators, Agency Access Control Administrators, or other designated personnel shall review and adjust access privileges when the role or responsibilities of a user changes or the user no longer needs access to County information systems or applications.

Unauthorized users to a system increases the risks of unauthorized disclosure and use of critical or sensitive information. CSB has not established procedures requiring periodic review of user lists to determine user appropriateness. Additionally, there was not process to notify the system administrator of changes to user access.

Recommendation: We recommend that CSB establish procedures requiring the appropriate staff to periodically review all of their system user lists and notify the system administrator when an employee is terminated, transferred or no longer authorized to use the systems. The access for all improper users should be removed. The review should be documented and initialed by the preparer and reviewer.

Management Response: Informatics staff will meet with CSB HR to establish written procedures for periodic review of user access to Credible and other information systems supported by the CSB. On a quarterly basis, CSB will compare Credible users with Active Directory and CSB HR Staff listings to identify any terminated staff that have not been properly disabled from access and send emails to supervisors requesting a review of staff rosters for contracted staff that no longer work for the CSB. Updates will be provided to the Informatics staff. The anticipated completion date is March 31, 2018.