# Fairfax County Internal Audit Office

**Health Department**
**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 separate report is being issued for each agency audited.

Health Department (HD) uses various systems to manage electronic medical records, pharmacy service, laboratory testing requests and etc. HD also uses Virginia Department of Health (VDH) systems to report/track communicable disease. We noted that Health Department data was identified and classified in accordance with the County Information Security policy and external regulations; user access rights were assigned based on job responsibilities; and, disclosure of data was properly authorized and complied with County policies and external regulations. However, we did identify exceptions where compliance and controls could be strengthened:

- Documentation supporting the request for user access or approval for access to applications with confidential/sensitive information was not retained for 5 sample systems.
- Periodic review of system user lists were not performed as required by Information Technology Security Policy 70-05.01 and HIPPA Security Rule (SR).

# 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 May 31, 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 the Health Department operates and determined the reasonableness of data classification. We selected a sample of information systems that stored confidential or sensitive information and conducted system walk-throughs to gain an understanding of the data stored in these systems. We performed user access rights test for these sampled systems 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.

We selected 10 systems from the Health Department for testing. All systems tested were classified as confidential.

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

## 1. User Access Authorization Forms

We noted that 5 of 10 sampled systems didn't use or retain user access request forms to support or evidence access approval granted. Prior to 2016, not all the HD systems were required to follow a formal user access authorization process to document approval before granting user access to the system. Starting late 2016, HD implemented the use of an electronic access request form stored on SharePoint to evidence request and approval of user access for most HD systems. However, we noted that not all the HD systems were listed on the electronic access request form. IAO was unable to obtain documentation verifying system user access authorization for users granted access prior to the implementation of the electronic access request process. Listed below are the systems and the number of users IAO found without supporting authorization documentation.

| System | Sample Tested | Users without authorization documentation |
|---|---|---|
| GE Centricity System | 2 (new users) | 2 |
| M Drive protected health information (PHI) folders | 20 | 12 |
| TB Investigation Contact Management Database | 10 | 5 |
| Avatar System | 25 | 18 |
| QS/1 Pharmacy System | 2 | 2 |

The Health Department is required to comply with DIT Security Policy 70-05.01 and HIPPA Security Rule (SR), which details requirements for handling electronic Protected Health Information (ePHI). HIPAA SR states:

- *Access Control: a covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information.*
- *Audit Control: a covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.*

DIT Security Policy 70-05.01 Section 3.5.2 Account *Administration* states:
*System Administrators or other designated staff:*

- *Requests for County information system accounts shall maintain a formal and valid access authorization based on approved intended system usage within personnel mission and business functions.*
- *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.*

Failure to properly document approvals for user access authorization of systems containing electronic Protected Health Information (ePHI) increases the risk of inappropriate use of protected information by users with unauthorized access.

**Recommendation:** The Health Department electronic access request form stored on SharePoint to document the system access authorization process should list all the systems HD uses. For the system users that were granted access prior to the adoption of the access request form, HD should ensure user access is valid and document the approval of their access during the department's periodic review of system user list. See the item #2.

**Management Response:** HD will add the missing systems onto its electronic access request form. The anticipated completion date is March 2018. During next user review, HD will document user access that was granted prior to the 2016 system authorization policy. Additionally, HD will work with Community Health Care Network (CHCN) contractor to set up tracking process for access to GE Centricity (EMR system used in our CHCN clinic sites). The anticipated completion date is May 2018.

## 2. Performance of Periodic Review of System Users

We noted that the system user access list for 7 of 10 sampled systems containing HIPAA ePHI, were not reviewed periodically to ensure users with access were appropriate. In 2 of the 7 systems we found active user accounts for individuals that no longer needed system access, these users should be removed from the system (see table below).

| System | Sample Tested | User should be removed |
|---|---|---|
| GE Centricity System | 11 | 1 |
| Avatar System | 25 | 1 |

The Health Department is required to comply with DIT Security Policy 70-05.01 and HIPPA Security Rule (SR), which details requirements for handling electronic Protected Health Information (ePHI). HIPAA SR states:
HIPPA Security Rule (SR) states:

- *Access Control: a covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information.*
- *Audit Control: a covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.*

DIT Security Policy 70-05.01 Section 3.5.2 Account *Administration* states:
*System Administrators or other designated staff:*

- *Requests for County information system accounts shall maintain a formal and valid access authorization based on approved intended system usage within personnel mission and business functions.*
- *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.*

Lack of periodic reviews of active user access for ePHI systems increases the risk of disclosure of Protected Health Information (PHI) to unauthorized personnel which increases the risk of misuse of protected information.

**Recommendation:** We recommend the Health Department perform a full review of all system user accounts, remove any improper users from any systems, and develop policy and procedures to periodically review users for all systems to ensure user access is valid. Documentation supporting the review of system users should be retained.

**Management Response:** HD has had policy in place for the review of system users, and performs regular reviews of the HIPAA-classified high/ medium risk systems. However, documentation requirements were not sufficient to meet the spirit of HIPAA and County 70-05 guidelines. These have been strengthened. System user reviews will occur every 6 months and documentation of review will be retained. For GE Centricity system, HD will work with CHCN technology contractor to ensure similar periodic reviews are in place and documentation is performed. The anticipated completion date is May 2018.