Office Of The City Auditor
Colorado Springs, Colorado

Denny L. Nester, City Auditor
MBA CPA CIA CFE CGFM CGAP

17-23 City of Colorado Springs Security of Fire Department Electronic Information Audit

November 2017

Purpose

The objective of this audit was to assess the processes and controls used by the Colorado Springs Fire Department (CSFD) to ensure the integrity and protection of critical electronic data. Special focus was given to HIPAA regulated Protected Health Information (PHI) and to Personally Identifiable Information (PII).

> *HIPAA regulated medical data, known as PHI, is all individually identifiable health information held or transmitted by a covered entity or its business associate in any form or media, whether electronic, paper or oral. PHI should be protected if the PHI identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Relevant rules are the HIPAA Privacy Rule[1] that covers PHI in any medium and the HIPAA Security Rule[2] that covers electronic protected health information.*
>
> *Personally Identifiable Information (PII) is defined as "any information about an individual …, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Relevant standards and guidance have been provided by the National Institute of Standards and Technology (NIST).[3]*

CSFD collects PII and PHI when providing services. Because information from CSFD closed incident reports can be requested via the Colorado Open Records Act and because CSFD shares PII and PHI with other agencies externally and internally with the City, it is imperative that adequate controls exist to protect this information.

[1]United States Department of Health and Human Services, Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996.
[2]United States Department of Health and Human Services, Security Rule to establish a national set of security standards for the protection of certain health information that is held or transferred in electronic form.
[3]NIST Special Publication 800-122, Guide to Protecting the Confidentiality of PII.

Highlights

Based on our review, we concluded that the processes and controls were mostly adequate for the needs of the organization. We noted twelve (12) observations, three (3) opportunities for improvement, and one (1) commendable practice that were discussed with the Colorado Springs Fire Department.

We are not including details concerning any potential vulnerabilities (or strengths) related to the security of the Colorado Springs Fire Department data. Disclosure of this information to the public would be contrary to the public interest in improving or maintaining secure electronic data for Colorado Springs Fire Department. The details of this audit are not required to be released to the public per C.R.S. § 24-72-204(2)(a)(VIII)(A).

Management Response

Management agreed to adequately address all observations with the exception of one observation due to staffing limitations. We will follow up on management's actions in future reports.

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing, a part of the Professional Practices Framework promulgated by the Institute of Internal Auditors.

City Council's Office of the City Auditor
City Hall, 107 North Nevada Ave. Suite 205, Mail Code 1542, Colorado Springs CO 80901-1575
Tel 719-385-5991 Fax 719-385-5699 Reporting Hotline 719-385-2387
www.ColoradoSprings.gov