City and County of Denver

201 West Colfax Avenue, Dept. 705 • Denver, Colorado 80202 • 720-913-5000 •
Fax 720-913-5253 • www.denvergov.org/auditor

Dennis J. Gallagher
Auditor

February 11, 2014

Michael Hancock, Mayor
Mayor's Office
1437 Bannock Street, Suite 350
Denver, CO 80202

Dear Mayor Hancock:

I am writing to bring your attention to a problem with the security of client files and employee records at Denver Human Services. This is a situation that requires immediate action to safeguard confidential information of Denver Human Services clients.

As you may be aware, one of my audit teams is finalizing the audit report of a comprehensive, citywide look at Denver's Identity Management processes. The audit assessed the effectiveness of internal controls used by Technology Services to manage and monitor system access to City information technology systems. The audit also is determining whether adequate controls are in place to protect vital records and confidential personal information; to ensure that that information is not at risk. Because of the confidential nature of the information they manage and the existence of regulations such as HIPAA that mandate that health information is appropriately restricted, Denver Human Services (DHS) has been one of the focal points of this audit.

Our audit work has found there are real security issues in the way DHS is managing access to their records and I am concerned that confidential personal information of DHS clients has been and continues to be at risk. For example, the audit team has found that a number of former employees of DHS have continued to have access to the agency's files, both physically and electronically after termination. Some of the physical rooms that former employees retained access to include the DHS records room, the Child Welfare office, and the DHS Human Resources file room. While our audit cannot ascertain if there was a breach of security regarding confidential records, the fact that unauthorized personnel had access to those records is very disturbing and represents a breach of public trust.

Moreover, DHS is not fully informed on which file rooms and system folders contain health and other confidential personal information and which do not. After the passage of multiple deadlines DHS has finally provided a partial list but is unable to provide even the most basic documentation that would show that they know where all confidential information is stored. For example, DHS has not been able to determine if confidential client records reside within a stated group of electronic file folders that former employees retained access to. The fact that multiple deadlines have come and gone and we are over a month out from this request shows either a terrifying lack of competency or a willful disregard for the request – a request made within my Charter-granted powers.

With the legal issue of access still unresolved my audit team has been careful ***not*** to request access to confidential client records. We've just asked for some assurance that DHS itself knows the places that confidential client information electronically resides and whether any breaches have occurred related to DHS clients as a result of unauthorized access.

If the potential security breach was not so concerning, I might find it amusing that the only entity that DHS seems to restrict from accessing client files is the Auditors Office.

While the audit has identified issues in other areas of the city, the issues related to DHS are of such immediate and critical concern that it prompts me to take this rare step of notifying you before the end of the audit so that you may immediately remedy these issues.

The following recommendations need to be immediately implemented to ensure that the information is safe.

- Determine where sensitive data related to clients and employees resides (both physically and logically).
- Perform a thorough review of all individuals with physical and logical access to sensitive data identified above.
- Disable or revoke access for those individuals that do require access to sensitive data.
- Retain evidence of any access reviews that are performed to assess the appropriateness of access.
- Ensure that sensitive data protected by rules and regulations is appropriately secured.

I hope you will react quickly to these recommendations and direct DHS to implement them ASAP to mitigate the risks that currently exist. Please let me know when these issues have been remedied.

For your information, this situation, and other findings from the Identity Management Performance Audit will be released at the March meeting of the Independent Audit Committee.

Sincerely,

Dennis Gallagher

Dennis J. Gallagher
Auditor

cc: Janice Sinden, Chief of Staff
Scott Martinez, City Attorney