

STATE OF CONNECTICUT



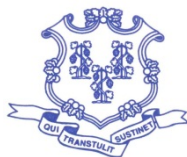
*AUDITORS' REPORT
DEPARTMENT OF ADMINISTRATIVE SERVICES
AVATAR SYSTEM
INFORMATION TECHNOLOGY SECURITY AUDIT
AS OF MARCH 2017*

AUDITORS OF PUBLIC ACCOUNTS
JOHN C. GERAGOSIAN ❖ ROBERT J. KANE

Table of Contents

INTRODUCTION	1
COMMENTS	2
FOREWORD	2
STATE AUDITORS' FINDINGS AND RECOMMENDATIONS.....	3
Data Transmission Integrity	3
Authentication Controls.....	4
User Account and Identifier Management	6
Logging of Changes to User Access Levels.....	7
Unsuccessful Login Attempts.....	8
Review of Audit Logs	9
Disabling of Inactive Accounts	10
Health Insurance Portability and Accountability Act (HIPAA) Policies	11
RECOMMENDATIONS	12
CONCLUSION.....	14

STATE OF CONNECTICUT



AUDITORS OF PUBLIC ACCOUNTS

State Capitol
210 Capitol Avenue
Hartford, Connecticut 06106-1559

JOHN C. GERAGOSIAN

ROBERT J. KANE

January 17, 2018

AUDITORS' REPORT DEPARTMENT OF ADMINISTRATIVE SERVICES AVATAR SYSTEM INFORMATION TECHNOLOGY SECURITY AUDIT AS OF MARCH 2017

We have audited certain operations of the Department of Administrative Services (DAS) Avatar System in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. The scope of our audit included, but was not necessarily limited to, the period ending March 2017. The objectives of our audit were to:

1. Evaluate the department's internal controls over significant management and financial functions;
2. Evaluate the department's compliance with policies and procedures internal to the department or promulgated by other state agencies, as well as certain legal provisions; and
3. Evaluate the economy and efficiency of certain management practices and operations, including certain financial transactions.

Our methodology included reviewing written policies and procedures, financial records, minutes of meetings, and other pertinent documents; interviewing various personnel of the department, as well as certain external parties; and testing selected transactions. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violations of contracts, grant agreements, or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our 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 such a basis.

The State Auditors' Findings and Recommendations in the accompanying report presents any findings arising from our audit of the Department of Administrative Services Avatar System.

COMMENTS

FOREWORD

The Department of Administrative Services operates primarily under the provisions of Title 4a, Chapter 57 of the Connecticut General Statutes.

Section 4a-1 of the General Statutes provides that the department head shall be the Commissioner of Administrative Services, who shall be appointed by the Governor. Melody A. Currey was appointed commissioner, effective January 7, 2015, and served in that position throughout the audited period.

The Department of Administrative Services, Collection Services Division and the Bureau of Enterprise Systems and Technology, administers the Avatar System. The primary responsibility of the Collection Services Division is to maximize revenue by billing, collecting and investigating claims for services provided by the Departments of Developmental Services, Social Services, Mental Health and Addiction Services, and Children and Families; whose facilities and programs span the state.

The Avatar system is a centralized billing system that DAS maintains on behalf of other state agencies. The system is used for processing and collecting bills, as a clearinghouse to ensure (a) compliance with the Health Insurance Portability and Accountability Act (HIPAA) regulations, and (b) identify funds reimbursable by Medicaid through the Department of Social Services.

STATE AUDITORS' FINDINGS AND RECOMMENDATIONS

Our review of the information technology control environment of the Department of Administrative Services Avatar System identified certain areas warranting attention, which are discussed in the following findings.

Data Transmission Integrity

Criteria: The National Institute of Standards and Technology (NIST) recommends implementing various controls to ensure data transmission integrity in its special publication 800-53 (SP 800-53). Control SC-8, Transmission Confidentiality and Integrity, requires the organization to:

- a) Implement cryptographic mechanisms to detect changes to information during transmission
- b) Cryptographic mechanisms* implemented to protect information integrity include, for example, cryptographic hash functions which have common application digital signatures, checksums, and message authentication codes

*Note: Cryptographic mechanisms are used to verify the authenticity of a piece of data. Two files can be assured to be identical only if the results generated from each file, using the same cryptographic (calculation) are identical.

Condition: During our review of the Avatar System data transmission integrity, we noted the following:

- The agencies, in their process of sending files to DAS to load into the Avatar System, do not provide any hash totals of the files they send.
- DAS does not calculate any hash totals on files received.
- The Avatar System does not compute any hash of each file before loading.

This presents a risk that the files sent by the agencies (for hospital services, etc.) might be corrupted during transfer and may go unnoticed. The files also may be manipulated or otherwise corrupted prior to loading. The ability to compare hashes upon receipt and load would help to ensure they are accurate, and would mitigate this risk.

- Effect:* Under the current process, the alteration, manipulation, or corruption of a file received from an agency may not be identified in a timely manner. Intentional manipulation or unintentional corruption of data during transfer might go unnoticed for a longer period of time than if hash functions were used to ensure file integrity.
- Cause:* The department has not explored the use of hash functions to ensure data transmission integrity for this purpose.
- Recommendation:* The Department of Administrative Services should use hash totals to ensure that files being loaded into the Avatar System have not been altered and agree with the original file received from each state agency providing hospital services. (See Recommendation 1.)
- Agency Response:* “The Department acknowledges the need to adhere to best practices for the secure transmission of data files. A project is pending to identify additional automation to introduce hashing/encryption which will reduce the risk of manipulation of data during file transport.”

Authentication Controls

Criteria: The National Institute of Standards and Technology (NIST) recommends various identification and authentication (IA) controls in its special publication 800-53 (SP 800-53).

Control IA-5, Authenticator Management, requires the organization to:

- a) Enforce minimum password complexity, including requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, and include minimum requirements for each criteria;
- b) Enforce a minimum number of changed characters when new passwords are created;
- c) Enforce password minimum and maximum lifetime restrictions; and
- d) Prohibit password reuse for a defined number of generations.

Condition: Password requirements in the Avatar application are currently configured as follows:

- a) Password length is currently set from a minimum of 4

characters to a maximum of 8 characters, both of which could be lengthened;

- b) Neither alpha nor numeric characters are specifically required, but could be;
- c) There is no special character requirement;
- d) There is no requirement on the number of times passwords can be reused;
- e) Passwords are not prohibited from including the employee's user ID, but could be; and
- f) The default password expiration is set to 999 days and could be shortened. In addition, there is a wide variation in the expiration rule for the current user accounts. Although 999 days was intended to be used for all accounts, the majority of account passwords are currently set to expire after 9,999 days, or 27 years. Consequently, in nearly all cases, they never expire.

Additionally, the Avatar data warehouse, often referred to as the "DSS (decision support system) database", contains a day-old copy of most database tables in the actual Avatar System, including tables having sensitive columns such as social security number and birthdate.

In this data warehouse, passwords may be reused any number of times, they do not expire, and there are no complexity requirements.

Effect: Authentication controls at the application and database levels are weak and could easily be compromised.

Cause: The department has not reviewed or considered the strength of the password policy for the Avatar System.

Recommendation: The Department of Administrative Services should take steps to strengthen its authentication controls related to the Avatar System to prevent unauthorized access to the system. (See Recommendation 2.)

Agency Response: "The Department agrees with this recommendation and is currently in the process of modifying password requirements to adhere to the End User Password Policy for Enterprise Standards developed by DAS/BEST."

User Account and Identifier Management

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) and identification and authentication controls (IA) in its special publication 800-53 (SP 800-53).

Control AC-2, Account Management, requires that organization-defined personnel approve requests to create information system accounts, and that each account's access to the information system be based on a valid access authorization.

Control IA-2, Identification and Authorization, requires that the information system uniquely identify and authenticate organizational users.

Condition: DAS did not provide Avatar System user access authorization forms for the current user population. Therefore, we could not confirm the justification or reasoning for the current user population, or determine who requested that each account be created, when the account was created, and what roles were authorized.

User accounts in Avatar are not associated with state employee ID numbers. The lack of correlation between user accounts and state employee numbers prevents the agency from automating account deactivation at termination.

In addition, at the time of our testing, the user descriptions (full names) associated with each user account contained the last names of 2 employees whose names have changed since their initial creation due to marriage and were never changed (neither their correct names nor their state employee ID numbers are stored in the system). In other cases, nicknames such as Jenny are used rather than Jennifer, making it difficult to identify the employee associated with each account.

Effect: The department's ability to validate the authorization of assigned access levels for its employees is impeded by the lack of documentation justifying each user's current access abilities.

The current system makes it difficult to identify which user accounts belong to which state employees because of the use of nicknames, maiden names, and other spelling variations. Also, there is an absence of uniquely identifying information such as each employee's state ID number.

Account deactivation for state employees cannot be automated, upon

termination, without recording each employee's unique state ID number.

Cause: DAS indicated that user access authorization forms are used and maintained. However, a recent move resulted in the misplacement of paperwork for all existing accounts.

At the time that the Avatar System was created, the unique Avatar usernames were not associated with each state employee ID number.

Recommendation: The Department of Administrative Services should reestablish the access levels of its current user population through new authorization forms to replace those that have been misplaced and store them electronically for backup purposes. Additionally, the department should associate or match Avatar usernames with Core-CT state employee ID numbers. (See Recommendation 3.)

Agency Response: "The Department agrees with this recommendation. DAS is in the process of developing a Footprint template for AVATAR user requests. This will keep all requests in an electronic format. DAS will generate new electronic requests for all current users when the Footprint template is available. The template will include state employee ID number which will be populated within the user definition form in AVATAR."

Logging of Changes to User Access Levels

Criteria: The National Institute of Standards and Technology (NIST) recommends various audit and accountability controls (AU) in its special publication 800-53 (SP 800-53).

Control AU-2, Audit Events, requires that the information system be capable of auditing organization-defined auditable events. The organization is to define those events that are significant and relevant to the security of the information system as audit events.

Changes to user access levels constitute events that are significant and relevant to the security of information systems.

Condition: The DAS audit trail does not capture changes to the Avatar System logical access restrictions. User role assignment is not tracked and only a user's current role is able to be determined at any given point in time. Therefore, the history of what role a user might have held in the past, and how long they held that role, is not recorded.

- Effect:* DAS is unable to analyze logs of changes to user access levels for suspicious activity, such as multiple changes in the same day or in a short time frame, because such logs are not generated.
- Cause:* Control logs are not maintained for the Avatar System.
- Recommendation:* The Department of Administrative Services should expand its audit trails to include changes made to the Avatar System user access levels. (See Recommendation 4.)
- Agency Response:* “The Department agrees with this recommendation. DAS is in the process of developing a Footprint template for AVATAR user requests which, when implemented, will allow for the ability to track changes made to user access levels.”

Unsuccessful Login Attempts

- Criteria:* The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53).
- Control AC-7, Unsuccessful Login Attempts, requires the organization to define and enforce a limit of consecutive invalid login attempts by a user during a specified time period and automatically lock out the user for a specified time period when the maximum number of unsuccessful attempts is exceeded.
- Condition:* Avatar System accounts are neither temporarily nor permanently locked out after a defined number of failed login attempts.
- This is a weakness at the application level only and not the database level, where accounts are locked out after 10 failed login attempts.
- Effect:* User accounts are more likely to become compromised if people are allowed an unlimited number of login attempts.
- Cause:* The Avatar application has the built-in functionality to lock out users after a set number of invalid login attempts. However, this setting was never enabled.
- Recommendation:* The Department of Administrative Services should enable account lockouts after a defined number of invalid login attempts to avoid unauthorized system access. (See Recommendation 5.)

Agency Response: “The Department agrees with this recommendation. DAS is in the process of updating AVATAR security defaults to enable account lockouts after a defined number of invalid logon attempts following the requirements in the End User Password Policy for Enterprise Standards developed by DAS/BEST.”

Review of Audit Logs

Criteria: The National Institute of Standards and Technology (NIST) recommends various access controls (AC) and audit and accountability (AU) controls in its special publication 800-53 (SP 800-53).

Control AC-2, Account Management, requires that the organization monitor the use of information system accounts.

Control AU-6, Audit Review, Analysis, and Reporting, requires the organization to review and analyze information system audit records for indications of organization-defined inappropriate or unusual activity and for those findings to be reported to organization-defined personnel.

Condition: Avatar System user activity is logged throughout several audit log tables. Although these audit log records are periodically reviewed, there is no standard procedure outlining what is to be done as part of those reviews, and the reviews are not documented.

Effect: Users could erroneously, unintentionally, mistakenly, or maliciously, alter data without oversight. Those alterations may not be detected in a timely manner.

Cause: DAS informed us that audit logs are reviewed, but no effort has been given to document those reviews or to formalize a process for what procedures should be performed as part of the reviews.

Recommendation: The Department of Administrative Services should establish procedures to define the specific steps that should be taken to review audit logs, the frequency of reviews, and how to document the steps that were performed. (See Recommendation 6.)

Agency Response: “The Department agrees with this recommendation. DAS will develop and implement procedures regarding the review of audit logs.”

Disabling of Inactive Accounts

- Criteria:* The National Institute of Standards and Technology (NIST) recommends various access controls (AC) in its special publication 800-53 (SP 800-53).
- Control AC-2 (3), Account Management, Disable Inactive Accounts, requires the organization's information system to automatically disable inactive accounts after an organization-defined time period.
- Condition:* The Avatar System does not automatically disable inactive accounts after any defined time period.
- At the time of our testing (May 2016), there were 36 active Avatar user accounts, 1 of which had never been used and 10 others that had not been used in over a year. Furthermore, of the 10 accounts, 8 had not been used in the last 5 years.
- These 11 accounts, comprising 31% of all accounts, would reasonably be defined as inactive.
- Effect:* Inactive accounts belonging to active employees present the possibility that these employees may not actually need access, unnecessarily allowing access to the system.
- It also presents the risk that others may attempt to log in as these users. Avatar also does not currently limit the number of invalid login attempts before locking an account (allowing for an unlimited number of attempts), which further increases this risk.
- Cause:* Part of the reason inactive accounts might exist is that users with little need to access the system have access. Additionally, last login times are not regularly evaluated.
- Recommendation:* The Department of Administrative Services should take steps to ensure that inactive Avatar System accounts are automatically disabled after a defined time period and that accounts are only created based on need. (See Recommendation 7.)
- Agency Response:* "The Department agrees with this recommendation, however, AVATAR does not currently provide the ability to automatically disable inactive user accounts. DAS will create a process to review inactive user accounts on a regular basis and manually disable as appropriate."

Health Insurance Portability and Accountability Act (HIPAA) Policies

- Criteria:* The HIPAA Security Rule, under section 164.316 (b) (2) (iii), requires that a covered entity review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.
- Condition:* The policies governing the Avatar System have not been updated or otherwise modified since their previous revision in November of 2004; the procedural documents have not been modified since their creation in May of 2004. Similarly, the last risk assessment of the system was conducted in March of 2005.
- Effect:* The policies and procedures that establish the foundation of governance for Avatar would not take into account improvements and changes to the operational and regulatory environment in which it operates.
- Cause:* DAS was not aware of the requirement to periodically review and update the HIPPA security rules.
- Recommendation:* The Department of Administrative Services should periodically review, and update as necessary, the governance documents for its Avatar System. A system-wide risk assessment should also be conducted regularly to account for potential new threats and vulnerabilities to the system. (See Recommendation 8.)
- Agency Response:* “The Department agrees with this recommendation. In compliance with the HIPAA Security Rule, DAS will periodically review, and update as necessary, the Security policies and procedures related to the Avatar System. A system-wide risk assessment will also be conducted on a regular basis.”

RECOMMENDATIONS

- 1. The Department of Administrative Services should use hash totals to ensure that files being loaded into the Avatar System have not been altered and agree with the original file received from each state agency providing hospital services.**

Comments:

We found that data files received by DAS are not hashed before or after they are received. Therefore, DAS cannot confirm that the files it loaded were not corrupted during the transfer or otherwise altered before, during, or after the transfer but before the loading of the data.

- 2. The Department of Administrative Services should take steps to strengthen its authentication controls related to the Avatar System to prevent unauthorized access to the system.**

Comments:

We found that Avatar System password controls and policies were weak.

- 3. The Department of Administrative Services should reestablish the access levels of its current user population through new authorization forms to replace those that have been misplaced and store them electronically for backup purposes. Additionally, the department should associate or match Avatar usernames with Core-CT state employee ID numbers.**

Comments:

We found that user access authorization forms for the current user population could not be provided by the agency because they misplaced the forms after a move between 2 office buildings. We also found that user accounts in Avatar are not associated with state employee ID numbers. This makes it difficult to determine the state employee that is assigned to each account.

- 4. The Department of Administrative Services should expand its audit trails to include changes made to Avatar System user access levels.**

Comments:

We found that the audit trail does not capture changes to logical access restrictions. Historical user role assignment and changes are not logged or recorded.

- 5. The Department of Administrative Services should enable account lockouts after a defined number of invalid login attempts to avoid unauthorized system access.**

Comments:

We found that at the application level, Avatar accounts are not locked out after any defined number of failed login attempts.

- 6. The Department of Administrative Services should establish procedures to define the specific steps that should be taken to review audit logs, the frequency of reviews, and how to document the steps that were performed.**

Comments:

We found that the Department of Administrative Services does not have standard procedures outlining how the audit log tables should be reviewed and how the audit log reviews should be documented.

- 7. The Department of Administrative Services should take steps to ensure that inactive Avatar System accounts are automatically disabled after a defined time period and that accounts are only created based on need.**

Comments:

We found that the Avatar System does not automatically disable inactive accounts after any defined time period.

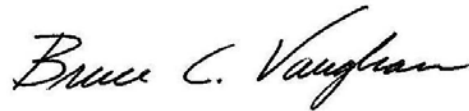
- 8. The Department of Administrative Services should periodically review, and update as necessary, the governance documents for its Avatar System. A system-wide risk assessment should also be conducted regularly to account for potential new threats and vulnerabilities to the system.**

Comments:

We found that the policies governing the Avatar System have not been updated or otherwise modified since their previous revision in November of 2004.

CONCLUSION

In conclusion, we wish to express our appreciation for the courtesies and cooperation extended to our representatives by the personnel of the Department of Administrative Services during the course of our examination.



Bruce C. Vaughan
Principal Auditor

Approved:



John C. Geragosian
Auditor of Public Accounts



Robert J. Kane
Auditor of Public Accounts