togetherforbetter

AUDIT REPORT

Social Service Implemented Adequate Information Technology Controls Over ACES, but There Are Opportunities for Improvement

October 2024

ANGELA DARRAGH, CPA, CISA, CFE
AUDIT DIRECTOR
CLARK COUNTY AUDIT DEPARTMENT

Audit Executive Summary

Social Service Implemented Adequate Information Technology Controls Over ACES, but There Are Opportunities for Improvement

October 2024

Background | Clark County Social Service provides care, support and relief to poor, indigent, incompetent, and elderly residents who are not eligible for other state, federal, or local programs.

Social Service utilizes a case management system to support participant intake, eligibility screening, client management, and financial management.

Bids for a new case management solution went out April 2006. A vendor was contracted in 2007 but ultimately was unable to perform the scope of work and the contract was terminated for convenience in 2012.

In June 2012, the Board awarded Curam Software, Inc. a contract to finish implementation and provide support for the case management system.

In 2014, the County's Automated Case Management System (ACES) went live as a customized implementation of the IBM Curam Social Program Management product. The County maintains ACES, periodically engaging the vendor for system enhancements and upgrades.

Objectives | We conducted this audit to evaluate the effectiveness of internal controls for ACES application and to identify any weakness or vulnerabilities that could compromise the confidentiality, integrity or availability of data within the system.

Summary and Key Findings | Overall, the ACES Information Technology application controls are reasonable.

The application has the correct automated benefit eligibility rules programmed in the financial assistance programs, patch management practices are appropriate, and some security controls have been developed.

However, user access reviews, user permission management, business continuity plans, data risk assessment, and administrator password change frequencies can be improved.

Recommendations | The audit report includes 15 recommendations including the following:

- Documenting and conducting periodic user access reviews;
- Performing a data risk assessment;
- Creating and implementing policies and procedures to periodically review ACES audit logs in high-risk areas

Details for each of those recommendations, along with others, are in the body of the report.

For more information about this or other audit reports go to clarkcountynv.gov/audit or call (702) 455-3269.

togetherforbetter

Audit Team

Angela Darragh, Director
Cynthia Birney, Audit Manager
Christopher Hui, Information System Auditor
Felix Luna, Principal Auditor
Tracy Banks, Internal Auditor

Audit Committee

Commissioner Michael Naft
Commissioner William McCurdy II
Commissioner Ross Miller

About the Audit Department

The Audit Department is an independent department of Clark County reporting directly to the County Manager. The Audit Department promotes economical, efficient, and effective operations and combats fraud, waste, and abuse by providing management with independent and objective evaluations of operations. The Department also helps keep the public informed about the quality of Clark County Management through audit reports.

You can obtain copies of this report by contacting:

Clark County Audit Department
PO Box 551120
Las Vegas, NV 89155-1120
(702) 455-3269

CountyAuditor@ClarkCountyNV.gov

Or download and view an electronic copy by visiting our website at:

https://www.clarkcountynv.gov/audit/Pages/AuditReports.aspx

Table of Contents

Background

The Clark County Department of Social Service provides care, support, and relief to poor, indigent, incompetent, and elderly residents who are not eligible for other state, federal, or local programs. The department is responsible for ensuring that Clark County meets its health, welfare, and community responsibilities pursuant to Nevada Revised Statues (NRS) Chapter 428 and Clark County Code of Ordinances Title 2, Chapter 2.48.

The primary mandates are to provide financial, home health aide assistance, long-term nursing care assistance, and burial/cremation assistance. Social Service is also responsible for other services and programs as assigned by the Board of County Commissioners. Table 1 describes some of the department's programs.

Table 1. Clark County Social Service Provides Various Programs to Help Those in Need

Program Name	Description
Burial and Cremation Services	Clark County is responsible for providing reimbursement to a contracted crematory, cemetery, funeral establishment, or direct cremation facility for the cremation or burial of indigent individuals who die within Clark County and who meet eligibility guidelines.
Financial Assistance	Financial assistance is provided for rent/mortgage, utilities, and other supportive services. An individual or household applying for financial assistance from Social Service must meet all eligibility criteria and participate in a case plan to attain self-sufficiency and /or sustainability.
Transportation Assistance	Social Service provides transportation assistance for indigent persons in Clark County to return to their resident state/county as required under NRS 428.080.
Homemaker Home Health Aide Program	The Homemaker Home Health Aide program provides assistance to seniors and disabled residents who need in-home support with grocery shopping, prescription pickup, laundry, light housekeeping, and meal preparation. Clark County Social Service contracts with private agencies for homemaker services.
Long Term Care	Social Service provides financial assistance and placement in adult day care and group care facilities

	and nursing homes to eligible residents who are unable to live independently. The program aims to preserve independence and ensure cost-efficient care is provided. Eligibility for long term care is determined by an assessment of need and pre-established eligibility criteria. All prior resource programs to assist with payment of long-term care are pursued prior to providing payment.
CARES Housing Assistance Program (CHAP)	The CARES Housing Assistance Program (CHAP) served residents of Clark County who suffered substantial financial hardship and lacked sufficient income or resources available to pay their housing costs because of the COVID-19 emergency or the response to that emergency. The program has evolved to now provides eviction prevention services and housing assistance to individuals on fixed income.

Note: The Department also provides other services including alternative health care, homeless outreach and coordinated intake, youth services and HIV/AIDS[1] assistance.
Source: Auditor prepared.

New Integrated Case Management System and Challenges During Implementation

Clark County Social Service utilizes a case management system to support the department's participant intake, eligibility screening, client management, and financial management The department's first case management system was developed in 1994.

The department's case management needs evolved since the implementation of the first case management system. Social Service was running a fragmented, non-integrated case management system, where many programs did not interact. Further, the department was using numerous databases outside the main system, performing redundant data entry, relying heavily on paper processes, and were unable to track provider referrals.

In April 2006, the County solicited bids for a new case management system to meet Social Service's evolving needs.

In September 2007, the County awarded a contract to Ciber, Inc. to implement a new case management system using the Curam Social Program Management software solution. Under this arrangement, Ciber acted as the integrator of the software solution built by Curam.

[1] Human Immunodeficiency Virus (HIV); Acquired Immune Deficiency Syndrome (AIDS)

The five-year Ciber, Inc. contract had a value of $6,594,548 for implementation, design, development, customization and initial support. Between September 2007 and March 2009, the Board approved several amendments to accommodate change requests. These amendments totaled $617,400.

In July 2011, Ciber, Inc. determined they would be unable to perform the full scope of work provisions outlined in the amended contract.

In March 2012, the Board approved the termination and settlement agreement with Ciber, Inc, with the company agreeing to provide consultation services to complete the project. At that time of termination, Ciber, Inc. had been paid $4.4M.

What is a Change Request?

A change request often arises when a client wants an addition or alteration to an agreed-upon deliverables for a project.

Change requests are often submitted during development and user acceptance testing before the final product is released.

In June 2012, the Board awarded Curam Software, Inc. a contract to finish implementation and provide support for the new case management system. This contract had a value of $4.9M. On July 1, 2013, International Business Machines Corporation (IBM) acquired Curam Software, Inc. and assumed assignment of the agreement.

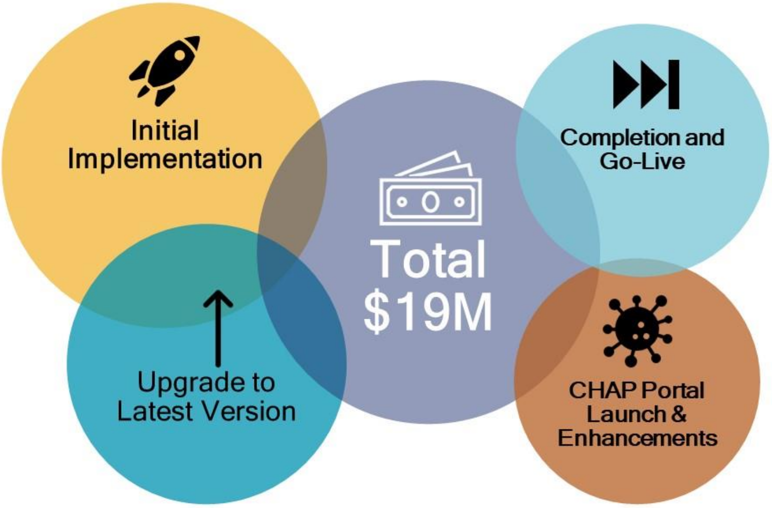
In 2014, the County's Automated Case Management System (ACES) went live as a customized implementation of the Curam Social Program Management product. The County has maintained ACES on its own, engaging IBM[2] periodically to assist with specialized system enhancements and upgrades.

Some of the major ACES enhancements and upgrades include a code upgrade in 2018 at a cost of $2.1M and several updates/additions as part of the County's COVID-19 emergency rental housing assistance program (CHAP[3]) launch. These CHAP updates/additions carried a cost of $6.3M paid for with federal pandemic funding. Figure 1 illustrates the total costs since the software application was implemented.

[2] In 2022, IBM divested and spun off their health and human services software division as Merative.

[3] We performed a separate audit of the County's CHAP program. That audit was issued in July 2024.

Figure 1. Clark County Has Spent $19M on ACES Implementation and Enhancements



Source: Auditor prepared

ACES facilitates the eligibility screening and acceptance of participants into the various Social Service programs. It also facilitates the ongoing maintenance of both the participant's eligibility for the program, and the supporting evidence for each application.

ACES Components and User Volume

Core ACES components include participant intake, eligibility, evidence processing, and participant management. ACES consists of the case worker portal and the citizen portal, which currently only serves the CHAP program. There are 210 active user accounts as of April 2024.

Clark County Social Service is part of the County's hybrid entity for HIPAA purposes (Health Insurance Portability and Accountability Act of 1996). The ACES application contains sensitive and privileged information, including information considered protected by HIPAA and Nevada Revised Statutes.

HIPAA Data and Penalties

HIPAA has three main rules that protect covered information: Privacy Rule, Security Rule and Breach Notification Rule.
A HIPAA violation occurs when a HIPAA-covered entity – or a business associate – fails to comply with one or more of the provisions of these rules. Table 2 lists 2024 HIPAA penalty structure.

Table 2. HIPAA Violations Carry Civil Penalties

Penalty Tier	Culpability	Minimum Penalty Per Violation - Inflation Adjusted	Max Penalty per Violation - Inflation Adjusted	Maximum Penalty Per Year (cap) - Inflation Adjusted
Tier 1	Lack of Knowledge	$137	$68,928	$2,067,813
Tier 2	Reasonable Cause	$1,379	$68,928	$2,067,813
Tier 3	Willful Neglect	$13,785	$68,928	$2,067,813
Tier 4	Willful Neglect (not corrected within 30 days)	$68,928	$2,067,813	$2,067,813

Source: HIPAA Journal. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

Maintaining proper internal controls over the data in ACES, and business processes helps to protect the information in custody of Social Service.

Objective

The objectives of our audit were to determine whether:

- Information technology application controls over the ACES software application, are effective and followed.
- Manual controls and/or internal processes are adequate to properly protect/safeguard client data, as well as maintain confidentiality, integrity, and availability of client data.

Conclusions

Overall, we found the ACES application controls are acceptable. The application has the correct automated benefit eligibility rules programmed in the financial assistance programs, patch management practices are reasonable, and some security controls have been developed.

However, user access reviews, user permission management, business continuity plans, data risk assessment and administrator password change frequencies can be improved.

Findings are rated based on a risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties. It also considers the impact on confidentiality, integrity, and availability of data.

6 Total Audit Findings

2 High Risk Findings

High risk findings indicate an immediate and significant threat to one or more of the impact areas.

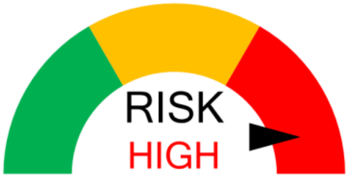
2 Medium Risk Findings

Medium risk findings indicate the conditions present a less significant threat to one or more of the impact areas. They also include issues that would be considered high if one control is not working as designed.

2 Low Risk Findings

Low risk findings are typically departures from best business practices or areas where effectiveness, efficiency, or internal controls can be enhanced. They also include issues that would be considered high or medium risk if alternate controls were not in place.

ACES Audit Logs Should be Routinely Reviewed



Social Service does not generate and review ACES audit logs[4] on a regular basis. Security audit logs are used as needed, but the department has not developed a formal review plan or strategy. Further, there is no documentation of how the current informal review is performed.

We believe the department should implement a formal strategy to review security related audit logs. This could include identifying questionable activity, creating a query to record these events, then pushing a report to appropriate personnel for review. Further, we believe there should be a logging and review strategy for high-risk transactions (*e.g., supervisory override*). These high-risk areas should be reviewed periodically for appropriateness.

The data in this application is covered by HIPAA and is also used to provide payment to clients. This data requires stringent protection of the data to ensure its confidentiality, integrity, and availability.

Federal regulations for review of audit logs are outlined in the Administrative Safeguards of the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(D) which states:

§ 164.308 Administrative safeguards.
(a) A covered entity or business associate must, in accordance with § 164.306:

> (ii) Implementation specifications:
>
> > (D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Section 164.312.(b) states:
§ 164.312 Technical safeguards.

[4] A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

A covered entity or business associate must, in accordance with § 164.306:

> (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

The National Institute of Standards and Technology[5] (NIST) guide[6] to computer security log management, section 2.2 states the following:

> “Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization’s internal investigations, establishing baselines, and identifying operational trends and long-term problems."

Civil monetary penalties for HIPAA violations can result in fines of between $137 and $68,928 per violation and compliance action plans that could include external monitoring. If a violation is found to be due to willful neglect, penalties can be as high as $2,067,813.

Recommendation

1.1 Conduct an accurate and thorough assessment of ACES to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data contained in ACES.

1.2 Create and implement policies and procedures to periodically review ACES audit logs in high-risk areas. At a minimum, this should include activities such as actions taken with administrative rights, including user creation, user activation, and permission changes.

Management Response

1.1 Assessment will be conducted with assistance of Clark County IT.

1.2 After an accurate and thorough assessment of ACES has been conducted to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data contained in ACES, then additional application centric logs will be created and implemented to address the risks and vulnerabilities delineated in the

[5] The National Institute of Standards and Technology is an agency of the United States Department of Commerce. They develop standards and regulations to improve the security and reliability of technology.
[6] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

assessment that are not covered in policies, and procedures.

ACES Risk Assessment Is Not Being Performed

Periodic security risk assessments[7] over the ACES software application are not being performed.

The last formal risk assessment was performed by the Clark County Information Technology department (IT) over five years ago. Clark County IT is currently conducting an overall risk and security assessment for HIPAA covered departments and HIPAA support departments. The performance of an ACES IT risk assessment is identified as a gap item for remediation. Responsibility for preparation of the assessment and gap mitigation is under discussion by Clark County IT and Social Service IT personnel.

Federal regulations for the performance of a risk assessment are outlined in the Administrative Safeguards of the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A) which states:

§ 164.308 Administrative safeguards.
(a) A covered entity or business associate must, in accordance with § 164.306:

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

There was no evidence of a practice to conduct recurring assessments of risk that included the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of data held by ACES.

Absence of a periodic risk assessment could increase the likelihood and magnitude and harm from unauthorized access, use, disclosure, disruption, modification or destruction of data maintain in ACES. This could result in litigation, regulatory noncompliance with potential fines for compliance violation, and reputation loss to Clark County. Civil monetary penalties for HIPAA violations can result in fines of between $137 and $68,928 per violation and compliance action plans that could

[7] An IT risk assessment is a process that helps organizations identify and evaluate potential threats to their information systems, networks, and data. The assessment also considers the possible consequences of these threats. The goal of an IT risk assessment is to reduce identified risks to avoid security incidents and compliance violations.

include external monitoring. If a violation is found to be due to willful neglect, penalties can be as high as $2,067,813.

Recommendation

2.1 Determine responsibility for performance of the ACES risk assessment.

2.2 Conduct an accurate and thorough risk assessment of ACES to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data contained in ACES.

2.3 Research gaps identified and design mitigation procedures based on results.

Management Response

2.1 Responsibility for the performance of ACES Risk Assessment is shared between Social Service technical team and Clark County IT.

2.2 The process of a yearly ACES Risk Assessment will be documented. Findings will be shared with Social Service management along with a mitigation plan of any identified gaps.

2.3 The yearly ACES Risk Assessment will include information related to gaps identified. Social Service technical team and Clark County IT will research applicable information and design mitigation procedures based on results.

Informal User Review Process Did Not Identify Accounts Needing to be Disabled

RISK
MEDIUM

Clark County Social Service, IT Administrators perform an informal quarterly review of the active accounts within the ACES software application.

This process involves asking division managers to verify whether the users (*employees*) continue to have a need for access and confirmation of their user role[8].

Although this user review is being performed, there is no documentation of the process, nor of the results of the review. In some instances, users are found with rights/roles that do not pertain to their current job duties.

We tested all 210 ACES user account as of April 2024 to determine whether the account's active status was warranted.

[8] A user role is a set of permissions and restrictions that define what a user can do within a software application. User roles can be assigned to users or groups of users based on their job title or other criteria.

We found 45 accounts (*out of 210*) that should have been disabled. This included former employees, generic user accounts and testing accounts as illustrated in Figure 2.

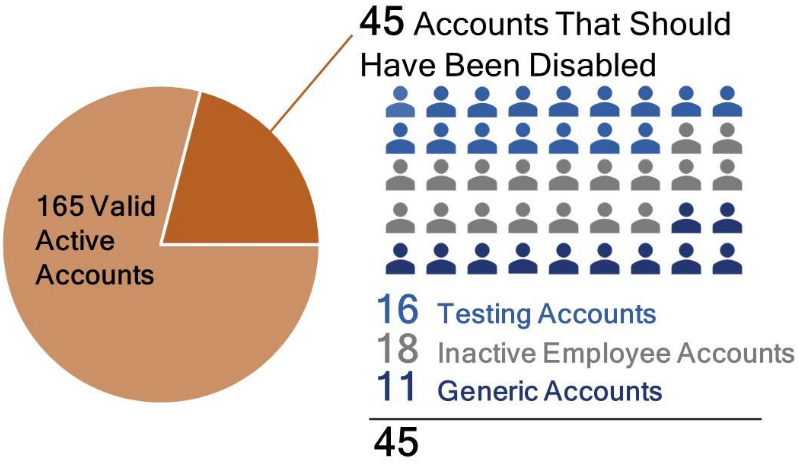


Figure 2. Majority of Active Accounts Warranted Active Status but Some Accounts Should Have Been Disabled
Source: Auditor testing

- **Testing Accounts:** 16 active accounts that are used for testing in the test environment. As a standard function, these accounts remain active in the production environment even after testing is completed in the test environment. These accounts should be disabled to reduce the risk of improper access.

- **Inactive Employee Accounts:** 18 active accounts pertaining to employees that are no longer with the County. Separation dates range from October 2019 to March 2024. These accounts were promptly removed once we notified Social Service IT Administrator.

- **Generic User Account**: 11 active accounts corresponding to a generic user. This account can be used by multiple persons and is usually needed for specific purposes. Once this purpose is no longer needed, the generic account should be disabled.

User access review, disabling of inactive employee accounts and generic accounts are outlined in Clark County Information Technology Directive Number 1:

> **C.1**
> User IDs must be disabled immediately for any individual who is no longer affiliated with the County or for any individual who has otherwise lost authorization for access to County Computing Systems and Networks. User IDs for employees of the County on a

leave of absence for prolonged personal or health reasons must be disabled on the first day of leave. The User ID will be reinstated upon official notification that the employee has returned from leave. User IDs that remain inactive for a period of time exceeding 60 days must be disabled. User IDs that remain inactive for a period of time exceeding 90 days must be deleted.

IV. C.2
The use of generic and guest accounts is not permitted. Individuals who require access to County Computing Systems and Networks must be assigned and must use a unique User ID with limited permissions. All default guest accounts must be deleted.

IV. C.2
User and Administrator permissions, which allow access to volumes, directories, and certain files, must be reviewed, and updated at least annually by the responsible Elected or Appointed Clark County Department Head.

The data in this application is covered by the HIPAA.

Federal regulations for unique user identification are outlined in the Administrative Safeguards of the HIPAA Security Rule, 45 CFR 164.312(a)(2)(i) which states:

§ 164.312 Technical safeguards.
(a) A covered entity or business associate must, in accordance with § 164.306:

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

The HIPAA Security Rule also address policies and procedures for granting access to protected information. Administrative Safeguards of the HIPAA Security Rule, 45 CFR 164.308(a)(4)(ii)(B) and 45 CFR164.308(a)(4)(ii)(C) state:

§ 164.308 Administrative safeguards.
(a) A covered entity or business associate must, in accordance with § 164.306:

(4)(ii) Implementation specifications:

(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a

> workstation, transaction, program, process, or other mechanism.
>
> (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Unused user accounts that remain active create a risk that the account can be compromised and used to perform transactions, resulting in a threat to the confidentiality, integrity, and availability of system data.

Recommendation

3.1 Implement policies and procedures for granting access to ACES per Technical Directive No.1 IV, C and maintain documentation for granting and changing user access.

3.2 Implement procedures and maintain documentation to ensure that when employees no longer need access to ACES, notification is provided to the Social Service IT department to disable accounts.

3.3 Conduct a user access review periodically and maintain documentation of review results.

3.4 If generic users are used, submit an exception form to Clark County IT, in accordance with Technical Directive No.1

3.5 Ensure testing accounts are disabled in the production environment.

Management Response

3.1 Policy and documented Standard Operating Procedure (SOP) will be implemented as per IT Directive No. 1. Policy and SOP will address granting ACES access through new CCSS Accessibility form.

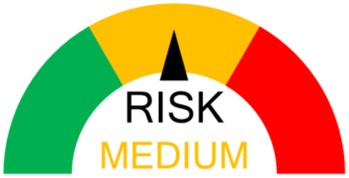
3.2 Policy and SOP will be updated to ensure accounts are being disabled timely. Documentation of changes to accounts will be stored in centralized location.

3.3 SOP will be created to include quarterly reviews of user access with results.

3.4 Exception forms will be submitted if/when generic users are used.

3.5 Process and procedure will be created to ensure testing accounts are disabled in production.

ACES Disaster Recovery Procedures Do Not Include Testing or Training



Social Service has an informal business contingency plan. This plan provides steps to take in the event of an unplanned incident and is centered around procedures to recover data in the event of a disaster and processes to continue serving program participants offline.

Part of the disaster recovery process includes utilizing a backup[9] of the ACES application. The ACES application data is routinely backed up and retained for several weeks.

Although the data is backed up, there is no formal testing of the backup image. Testing would reveal whether the data is usable and reliable should there be a need to utilize the backup. An infrequent test is performed when the ACES test environment is refreshed but this event does not happen on a routine basis.

While the department has developed a business contingency plan, the plan is informal and there is no training on how to engage the plan, should there be a need. These steps are generally known among current staff but not documented for reference. Further, there is no testing of the overall business contingency plan to ensure the plan goals would be achieved.

The HIPAA Security Rule addresses disaster and contingency plans. Administrative Safeguards of the HIPAA Security Rule**,** 45 CFR 164.308(A)(7)(i) states:

§ 164.308 Administrative safeguards.
(a) A covered entity or business associate must, in accordance with § 164.306:

> (7) (i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Lack of written documentation on all facets of the business contingency plan could result increase time to reestablish essential business functions during an unplanned disaster.

[9] A copy of files and programs made to facilitate recovery if necessary.

Lack of training and testing of the business contingency plan could result in staff not knowing their roles and responsibilities in the event of a disaster. Both of these could result in violations to HIPAA and civil monetary penalties.

Recommendation

4.1 Finalize and document the Business Contingency Plan. Once established, conduct annual reviews, testing and training of the plan.

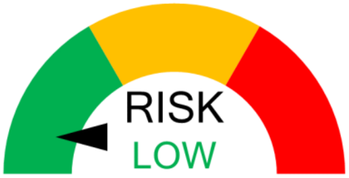
4.2 Include a periodic backup data testing in the disaster recovery plan. Periodically test this data and document the results of the testing.

Management Response

4.1 Social Service will develop a Business Contingency Plan addressing required duties related to business practice and establishing roles and responsibilities throughout the department to ensure critical need services are available. Plan will include dates for annual review, routine testing and training as well as documentation of completion.

4.2 Annually, data will be restored from backups to a non-production database environment. Following this, the DBA team will generate a validation report that juxtaposes the restored database with the current production database, comparing both table and row counts across these two environments. Subsequently, Social Service and the application support team will execute a standard set of regression test cases to verify the operational status of the restored database. A comprehensive report of these results will be generated and archived in the Service Now system.

Approval Forms Were Completed after Permissions Were Provided



We identified 50 privileged[10] users for the ACES software application as of April 2024. These accounts are considered

[10] A privileged account is a user account that has more access rights and permissions than a standard account.

privileged accounts because they contain rights[11] that allow users the options to perform functions that would normally be reserved for system administrators and supervisory staff. This can include approving payments, assigning supervisory tasks etc.

Social Service IT Administrators rely on a paper access to grant ACES system access based on what is indicated on the form. This form is comprehensive and indicates management approval for the access being requested. There is a form for account creation and one for changing rights (*e.g., when an employee moves from one office to another or promotes to a supervisory position*).

We used professional judgement to select 26 users with privileged rights (*out of 50 total privileged users*) and found the following:

- **Access form completed after privilege granted:** We identified 11 privileged user accounts (*out of 26 sampled*) that had paper approval forms on file, but the approval dates (*on the paper forms*) were after roles were granted in ACES.

- **System access did not match access form:** 2 privileged user accounts (*out of 26 sampled*) where the paper form did not agree with the privileged right granted. We believe the forms were filled out incorrectly.

- **No Account Creation Form:** 3 privileged user accounts (*out of 26 sampled*) did not have account creation access forms available for review. Of the three, two did have a change form available, but one had neither an account change form nor an account creation form on file.

Overall, we believe there is room for improvement with managing the access forms. Clark County Information Technology Directive Number 1 requires system access to be approved by a department director or designee. Having the forms on file evidence that this requirement was met.

There is a risk that privileged users may be granted inappropriate access, resulting in risks to the confidentiality, integrity, and availability of system data.

[11] User access rights, also known as permissions or privileges, are the levels of access granted to users within an organization to interact with specific features, data, or functionalities of a software platform.

Recommendation

5.1 Provide supervisory staff and management with a periodic reminder that access forms are required when users are created, move location or require privileged rights.

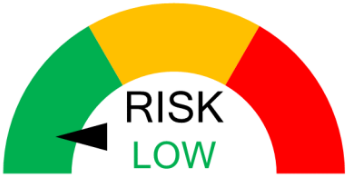
5.2 Do not grant privileged ACES system access until after a form is completed and approved. Retain paper forms in a central location for future reference as needed.

Management Response

5.1 New Social Service Accessibility form and accompanying training is currently under development, Accessibility form will be required for new staff, when users are being moved, and when privileged rights are required.

5.2 SOP will be developed outlining access will only be granted once all needed forms are received. Forms will be stored in centralized location for future reference.

ACES Administrators Do Not Change Passwords Every 45 Days as Required by County Technology Directive No.1



Although regular ACES user accounts must change passwords every 90 days (*due to integration with Active Directory*), we found that ACES administrator accounts are currently not changing their password every 45 days, as required by Clark County Technology Directive Number 1. This directive states:

Information Technology Security Policy (Technology Directive No. 1 (TD No. 1))
IV. PROCEDURE
C. System Access Control
2. Administrator passwords must be changed every 45 days and must never be reused.

Changing administrator account passwords is more critical than regular users. If an attacker gains access to an administrator's password, the application's infrastructure and data is at significantly greater risk.

Currently, ACES cannot differentiate password requirements for administrators and general users, so the more lenient requirement was applied to all users. A solution is being explored as of April 2024.

Recommendation

6.1 Establish procedures for administrators to manually change their password every 45 days or change the system parameter to require all administrator passwords be changed every 45 days.

Management Response

6.1 If ACES users with administrator roles are not already part of a specialized Active Directory group, one will be created, and these users will be added to it. Subsequently, a group policy will be implemented to ensure that passwords for users in this AD group expire every 45 days. The ACES support team may need to develop a program to identify individuals with ACES administrator roles who are not in the AD group. Upon identification, a notice will be sent to Social Service to request the addition of these users to the AD group.

Appendix A: Audit Scope, Methodology, and GAGAS Compliance

Scope

The audit covered the period from October 12, 2020, through July 1, 2023, through March 27, 2024. The last day of field work was June 10, 2024. This audit was performed as part of our audit plan.

Methodology

To accomplish our objectives, we performed a preliminary survey where we gathered background information, reviewed the history of the automated case management system project, reviewed applicable laws and regulations, and interviewed staff and management. We then identified risks relevant to our audit objective.

Based on the risks identified during our preliminary survey, we developed an audit program and then performed following procedures:

- Obtained the ACES software application and database user list and then:
  - Reviewed all users (total of 210) to determine whether access to the application and database was warranted based on their employment status.
  - Determine whether generic and testing accounts are disable in the production environment of the ACES software application.
- Identified privilege users (50 total) and then used professional judgement to select 26 of those users. For each selected privileged user, we determined whether access was warranted by reviewing the access form and/or confirming with management.
- Reviewed the most recent disaster recovery and business contingency plan to determine whether the plans are in written form, detailed, include procedures for when system is down, inclusive of employee responsibilities, periodically tested and plan training is performed.

- Interviewed staff involved in disaster recovery to gauge their familiarity with indicated processes and their overall familiarity with the plan.
- Reviewed the ACES patch management procedures to determine if they include and/or indicate:
  - Staff responsible for the patch management process.
  - Authorization and testing of patches prior to installation.
  - Process for relaying bugs/errors to application vendor.
- Interviewed staff and reviewed meeting minutes to determine whether ACES patches are performed based on the vendor's recommendation and/or as needed. Also, whether patches are tested prior to installation in the production environment.
- Reviewed the ACES standard and privileged user password configuration settings to determine whether password change frequency, complexity and length meet Clark County Information Technology Directives.
- Interviewed staff and reviewed ACES/Curam system manuals to determine whether encryption practices for transmitted data (*internally/externally*) and data at rest are in alignment with NIST standards and HIPAA requirements.
- Reviewed the ACES sign on configuration to confirm that access is integrated with Windows Active Directory and access to the worker portal is restricted outside of the County domain.
- Reviewed the ACES system manuals to determine whether the application is capable of logging security events and logging is comprehensive enough to detect improper activity.
- Performed case workflows in the ACES testing environment to determine whether:
  - ACES was properly computing eligibility for financial assistance programs based on household size, household income, household resources and specific program eligibility criteria.
  - CHAP payment could not be approved by regular user and required supervisory authority.
  - mock scenarios with Social Service IT to test eligibility rules programed within ACES for Financial Assistance and CHAP housing assistance.
  - Supervisory approval workflow was working as designed.
  - Financial case workflow could not proceed without the requisite user input.
- Interviewed staff to determine whether a HIPAA IT data risk assessment is being periodically performed.

While some samples selected were not statistically relevant, we believe they are sufficient to provide findings for the population as a whole.

Our review included an assessment of internal controls in the audited areas. Any significant findings related to internal control are included in the detailed results.

Standards Statement

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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. Our department is independent per the GAGAS requirements for internal auditors.