

Mental Health Management System (Welligent) Audit

Mental Health Management System (Welligent) Audit

Table of Contents

Executive Summary	3
Background	3
Scope	4
Objective.....	4
Methodology.....	4
Audit Observations and Recommendations.....	6
Observation 1 – Further controls for restricting user access and associated authorizations and privileges should be implemented.....	7
Conclusion.....	9
Attachment 1	10
Definition of Risk Level	10
Attachment 2	11
Management Response	11

Date: February 14, 2024

To: Board of Trustees
Stephanie S. Elizalde, Ed.D., Superintendent

From: Robert Rubel, MBA, CPA, CIA, CISA
Chief Internal Audit Officer

Subject: Mental Health Management System (Welligent) Audit

Executive Summary

The Dallas Independent School District (District) Office of Internal Audit (OIA) has completed the Mental Health Management System (Welligent) Audit.

The audit focused on the District's processes and controls over data maintained in Welligent, a cloud-based electronic health records (EHR) system. The audit included reviewing application controls surrounding user access, data accuracy, validity, and history, as well as data security and privacy, to determine if appropriate based on federal, state, and local policies, as well as industry best practices determined by the National Institute of Standards and Technology (NIST).

Welligent is overseen by the Mental Health Services (MHS) department. The platform is used to process sensitive student data that must comply with both FERPA and HIPAA privacy laws, and as such, it is crucial that controls are in place to ensure this data is accurate, reliable, and protected. One of the most effective and efficient ways to do this is through system automated controls. If automated system controls cannot be utilized, then other manual and monitoring controls should be implemented.

Overall, MHS has done an excellent job to implement a functional system with strong application controls to mitigate risks such as data accuracy, reliability, and privacy.

An opportunity for improvement was identified in the following area:

1. Further controls for restricting user access and associated authorizations and privileges should be implemented.

Background

MHS offers mental, behavioral, and physical health services across 240 district campuses as well as 13 off-site clinics. The department provides resources to improve the health and wellbeing of students and personnel within the District through its various clinic and school-based programs. Both clinic-based and school-based programs offer services such as therapy and psychiatry.

MHS partnered with and implemented Welligent in January 2023 to help manage and track student health records, services provided, as well as any billings for Medicaid reimbursements. The security of the data maintained in Welligent is a shared responsibility between the vendor and the District. A data sharing agreement was entered into with Welligent to provide protection for the data maintained on their cloud-based server; however, it is still the responsibility of the District to ensure the data is accurate, complete, and properly restricted, as everyone with access

to the data affects whether it remains safe.

Welligent's main users consist of the following roles:

- Clinicians – Provide billable and non-billable mental health services to students both on site at campuses and at offsite clinics. Their job functions require them to add programs, services, and enter session notes in Welligent for services performed.
- Licensed Psychiatrists – Have a similar role as clinicians, but they provide billable services to students only at clinics.
- Managers – Located both in clinics and schools, administratively helping clinicians provide services and have more access in Welligent compared to the role of clinicians.
- Administrative Assistants – Located only at the clinics their responsibilities are broad, such as coordinating communications between clinics and parents, adding programs or services for students, and scheduling appointments for students to receive services.
- Wraparound Specialists – Coordinates with school, clinic, and families to facilitate services.
- Billing Specialists – Responsible for submitting claims for Medicaid reimbursement.
- Data Analysts and MHS Leadership¹ – Monitor the overall performance of MHS.

MHS has processed 52,626 services for 8,786 students in Welligent between January 2023 and September 2023. Referrals for services can originate from parents, counselors, principals, or students themselves and can be submitted online, in person, or by phone. Once a referral is made, a student profile is created in Welligent where all documentation such as consent, services received, appointments, session notes, etc. is maintained. The department has various medical, professional, and ethical standards it must meet to ensure the best care is provided to patients. The platform has been instrumental in managing that standards are met, and services are effective.

Scope

The audit focused on current application controls within Welligent along with related data for fiscal year (FY) 2022-2023 and FY 2023-2024.

Objective

The objective of the audit was to review the processes and application controls surrounding data maintained in Welligent.

Methodology

OIA reviewed processes, controls, and supporting documents related to data maintained in

¹ Executive Director, Directors, and Quality Assurance Manager

Welligent. Auditors interviewed key personnel, conducted walkthroughs, and performed the following:

1. User Access — To determine whether mental health data maintained within Welligent is properly restricted, auditors performed the following:

- Auditors reviewed login configurations in Welligent to determine the following:
 - Password requirements met best practice standards for length and complexity.
 - Two-factor authentication is in place.
 - Automated lock-out after prolonged inactivity

See Recommendation 1 in this report.

- Auditors obtained a user access listing from Welligent as of September 20, 2023, totaling 218 users. Auditors compared the listing to an active employee listing generated from Oracle to verify users were currently employed by the District. No observations were noted.
- Auditors obtained access logs from September 1, 2023, to September 20, 2023, and verified only authorized users accessed the system. No observations were noted.
- Auditors obtained and reviewed role-based user authorizations and privileges within Welligent to determine if access to data and system functions were appropriate based on job duties and verify if proper segregation of duties were in place. Auditors then selected 20 employees from the user access listing to verify the role assigned in Welligent was appropriate based off their job titles and locations in Oracle.

See Recommendation 1 in this report.

- Auditors obtained a listing of users that had administrative rights in Welligent to verify administrative access was properly restricted and appropriate based on job functions.

See Recommendation 1 in this report.

2. Data Modifications – To determine if controls are in place to properly track and monitor data modifications, auditors first reviewed the department's processes to determine fields that contain high-risk data. Auditors then determined if audit logs were maintained for the determined high-risk data fields. Finally, auditors obtained the audit logs for program history and medication history from September 1, 2023, to September 25, 2023, to test if audit logs were properly retained and modifications were appropriate. No observations were noted.

3. Data Accuracy and Validity — To determine if application controls are in place for verifying the accuracy and validity of data maintained in Welligent, auditors conducted the following:

- Auditors created test cases, as both clinic-based personnel and campus-based personnel, and walked through MHS processes in Welligent to determine if the following automated controls are in place where applicable:
 - Required format field checks

- System sequencing checks
- Automated validations
- Error messages

No observations were noted.

4. Vendor Agreements — To determine if Welligent has policies in place that address their controls for mitigating risks such as data loss, theft, recovery, etc., auditors obtained the most recent service agreement and data sharing agreement and verified they address data privacy, security, backup/recovery, and compliance with applicable regulations. To test if the vendor is in compliance with the agreements, auditors conducted the following:

- Auditors obtained and reviewed documentation for the three most recent incident responses and determined if incidents were properly documented (e.g., persons involved, date and time the incident occurred, escalation method, steps taken), and appropriate steps were taken on any exceptions noted.
No observations were noted.
- Auditors obtained and reviewed the most recent penetration testing results to determine if penetration testing was performed.
No observations were noted.
- Auditors obtained and reviewed supporting documentation of a recent vulnerability scan to verify vulnerability scans were performed.
No observations were noted.
- Auditors obtained and reviewed the patch management schedule along with supporting documentation to verify the last patch was performed successfully.
No observations were noted.
- Auditors obtained and reviewed supporting documentation of the most recent data backup to determine if backup was successfully completed.
No observations were noted.
- Auditors requested the most recent Service Organization Controls (SOC)² report to determine if the vendor has been evaluated by an independent party.
No observations were noted; however, results were communicated to MHS for review.

Primary criteria used for this audit were:

1. National Institute of Standards and Technology (NIST) Security and Privacy Controls for Information Systems and Organizations, September 2020
2. Federal Information System Controls Audit Manual (FISCAM), February 2009

Audit Observations and Recommendations

² A Service Organization Controls (SOC) report provides independent validation over a company's internal reporting controls and a SOC 2 report puts a higher focus on the cybersecurity aspect of an organization. This includes information security, availability, process integrity, confidentiality, and privacy controls.

Observation 1 – Further controls for restricting user access and associated authorizations and privileges should be implemented.

Condition

Auditors reviewed controls for restricting user access as well as user authorizations and privileges within Welligent and noted the following:

- Administrative access could be further restricted.

Auditors reviewed the current listing of MHS administrator roles in Welligent noting a total of 12 administrators. Auditors reviewed the users with MHS administrator access noting six of the users did not have job functions aligned with that of a system administrator.

- Access controls could be strengthened.

When reviewing the process for granting access to Welligent, auditors noted access is currently granted via a manual process where users make a request to the MHS system administrators via email. The administrators are responsible for granting type of access and associated authorizations and privileges, which is based on the user's role. When a user changes roles or is terminated from the system it is also a manual process to notify the administrators that access needs to be changed or revoked. Additionally, the administrators are responsible for setting up password configurations for each user as access is not linked to the District's Single Sign-On method, Rapid Identity. Auditors noted two-factor authentication is offered in Welligent but is not selected as a part of the user's password configurations.

- User authorizations and privileges could be further restricted.

Auditors reviewed the role-based authorizations and privileges for Welligent users noting there were thirteen roles set up in the system. Auditors reviewed the department's processes to determine appropriate authorizations and privileges based on job functions, segregation of duties, etc. Auditors noted the following instances where user authorizations and privileges may not be appropriate:

- The role of billing specialist has the ability to edit session notes, which is a function that should only be performed by clinicians.
- Additionally, the role of clinic managers and school-based managers are configured to grant access to other users, where best practices would configure only the administrator role to have these rights.

Cause

Given the short period of time since Welligent has been implemented, MHS has done a good job of setting up role-based authorizations and privileges. The department, however, has not yet had time to fully review and adjust user access and role-based authorizations and privileges to ensure the strongest controls are implemented as the primary focus is to get the operating system functioning properly for end users.

Effect

Insufficient controls surrounding user access and associated authorizations and privileges can lead to an increased risk of unauthorized or inappropriate access and/or changes to sensitive student data.

Recommendation 1

To strengthen controls surrounding user access and associated authorizations and privileges, MHS should consider the following:

- Restrict administrative access to a few select individuals that should have permission to administer the system and the data it maintains. Additionally, restrict the ability to add users to only those with administrator rights.
- If viable, link Welligent to Rapid Identity to enhance security and streamline user access processes. A process to periodically review user access should still be implemented as user roles will change and terminated users will need to be archived within Welligent; however, terminated users' access will be automatically restricted significantly reducing the risk of unauthorized access to sensitive data.
- Update the billing specialist role to remove the ability to modify session notes.
- Document criteria, processes, and procedures for granting user access and associated authorizations and privileges based on job functions, segregation of duties, etc. and implement a process to review periodically for appropriateness.

Criteria

National Institute of Standards and Technology – Security and Privacy Controls for Informational Systems and Organizations IA-5 Authentication Management, September 2020

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances.

National Institute of Standards and Technology – Security and Privacy Controls for Informational Systems and Organizations SC-2 Separation of System and User Functionality, September 2020

Preventing the presentation of system management functionality at interfaces to non-privileged users ensures that system administration options, including administrator privileges, are not available to the general user population. Restricting user access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information.

National Institute of Standards and Technology – Security and Privacy Controls for Informational Systems and Organizations AC-6 Least Privilege, September 2020

Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. Organizations should restrict privileged accounts to specific personnel or roles to prevent day-to-day users from accessing privileged information or privileged functions.

Risk Level for Observation 1: Medium³

Conclusion

Welligent is utilized by MHS to track, monitor, and bill mental health services provided to students. As the system houses sensitive data, it is crucial that application controls are implemented to accurately track, monitor, and safeguard student data.

Overall, MHS has done an excellent job to implement a functional system with strong application controls to mitigate risks such as data accuracy, reliability, and privacy. Implementation of the recommendations in this report would improve the overall security and confidentiality of student data maintained in Welligent.

We would like to thank MHS and the Welligent team for their cooperation and assistance with this audit.

The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Those standards require OIA to plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our observations and conclusions based on our audit objectives. OIA believes the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

Respectfully submitted,

Robert Rubel

Robert Rubel, MBA, CPA, CIA, CISA
Chief Internal Audit Officer

Cc: Pamela Lear, Ed.D., Deputy Superintendent, Chief of Staff and Racial Equity Officer
Sherry West, Deputy Chief, Chief of Staff
Tracey Brown, Executive Director I, Mental Health Services, Chief of Staff
Concepcion Rodriguez, Director II, Operations, Mental Health Services, Chief of Staff
Annmarie Perez, Quality Assurance Manager, Mental Health Services, Chief of Staff

Acknowledgments:

Eva Narten, CPA, CIA, CISA, Deputy Chief, Internal Audit
Shelly Kelley, CPA, Audit Director II
Richard Siu, CIA, Audit Manager
Claire Chen, CPA, CISA, Auditor II
Osvaldo Alonso, CFE, Auditor II

³ See Attachment 1 for Definition of Risk Level.

Definition of Risk Level

Risk Level	Definition
High	High probability of occurrence that would significantly impact District operations and have a significant financial or compliance risk. These observations are defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of the District.
Medium	Risks are considered to be substantially undesirable and pose a moderate level of risk exposure to District operations. Without appropriate controls, the risk will happen on a consistent basis.
Low	The risks are considered to be undesirable and could moderately expose the District. Without appropriate controls, the risk will occur some of the time.

Management Response

Observation 1 – Further controls for restricting user access and associated authorizations and privileges should be implemented.

Acknowledgement of observation:

- ☒ Agree
- ☐ Disagree

Management's Response:

All changes have already been implemented except for two-factor and multi-factor (rapid identity) authentication.

Welligent two-factor authentication will be implemented in January 2024 for all MHS staff. Two-factor authentication has already been implemented for the Quality Assurance manager.

Multi-factor authentication will be implemented once SSO technology is available in Welligent. They anticipate it will be ready the end of the first quarter, 2024. Once this technology is available in Welligent, MHS will work with the Dallas ISD Edtech-Architecture team to implement rapid identity technology. The Edtech team will need to test the technology prior to it going live. The anticipated implementation date will be May 2024 but may need to be adjusted, if Welligent has a delay in its availability.

Estimated Implementation Date:
May 31, 2024

Individuals responsible for implementation:

Tracey Brown, MHS Executive Director, Annmarie Perez, MHS Quality Assurance Manager, Edtech-Architecture, and their Operations staff. Will need guidance from Welligent analysts.