

Health Services Records IT Controls Audit

Health Services Records IT Controls Audit

Table of Contents

Executive Summary	3
Background	3
Scope	6
Objective	6
Methodology	6
Audit Observations and Recommendations	9
Observation 1	9
Conclusion.....	11
Attachment 1	12
Definition of Risk Level	12
Attachment 2	13
Management Response.....	13
Attachment 3	15
Criteria by Observation	15

Date: April 29, 2026

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

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

Subject: Health Services Records IT Controls Audit

Executive Summary

The Dallas Independent School District (District) Office of Internal Audit (OIA) has completed the Health Services Records IT Controls Audit.

The audit focused on the processes and information technology controls surrounding the District's electronic health records system hosted by August Schools (August) including user access management, data accuracy and validity, data security, and compliance with policies and applicable regulations. A well-designed and effectively managed electronic health records system promotes accountability, supports operational readiness, and helps ensure regulatory compliance.

Overall, Health Services has implemented controls to ensure the accuracy and validity of health data, safeguard data security, and maintain compliance with District policies and applicable regulations.

Opportunities for improvement were identified in the following areas:

Observation	Priority	Recommendation
1	Medium	Complete establishing automated August system interfaces, renegotiate contract terms, enhance security settings, update the service level agreement with measurable benchmarks, and implement standardized incident documentation.

Implementation of the recommendations in this report would assist Health Services to enhance the effectiveness and efficiency of its electronic health records system processes.

Background

Health Services

The District's Health Services Department (Health Services) collaborates with school staff, parents, and the broader community to improve student wellness by maximizing access to health-related resources. The department currently employs over 300 healthcare professionals to support campus clinic operations. Each campus is staffed with a full-time nurse, while nurse assistants provide support across multiple campuses on an as-needed basis. Additionally, there are 40 central office staff supporting districtwide health initiatives.

Health Services oversees a broad range of responsibilities, including monitoring immunization compliance, tracking communicable diseases, documenting results from state-mandated screenings, and most importantly, providing treatment to students in need.

Immunization Requirements

State law requires public school districts to maintain up-to-date immunization records for each enrolled student and to annually report the immunization status of students in kindergarten and seventh grade. The immunization report must be submitted electronically by the District between the last Friday in October and the second Friday in December. Required data elements include total enrollment counts for kindergarten and seventh grade, the number of students with conscientious exemptions, the number with medical exemptions, and the number of students without immunization records on file.

State regulations permit provisional enrollment for students who have received at least one dose of each required vaccine. For these students, a school nurse or administrator must review immunization status every 30 days to confirm continued progress toward full compliance. If, at the end of the review period, a student has not received the next required dose, they may submit an applicable exemption form (e.g., medical or conscientious). Otherwise, the student is considered noncompliant and must be excluded from school until the required vaccination is administered.

To meet statutory requirements, the District uses August as its primary system for tracking student immunization status. August centralizes immunization data, displays individual compliance status, and generates districtwide reports identifying students as compliant, noncompliant, or exempt. The system also maintains documentation of follow-up activities and provides template forms for parent communication.

Health Services maintains centralized oversight through nurse supervisors assigned to designated regions across the District. Nurse supervisors generate regional immunization status reports from August every 30 days and notify campus nurses of students requiring follow-up. Campus nurses may issue notification letters to parents and upload documentation into August as evidence of outreach efforts.

Screening Requirements

State law requires public school districts to conduct mandatory student health screenings each year such as vision, hearing, and spinal screenings to identify conditions that could affect learning or overall well-being. Districts must complete these screenings within required timelines and submit annual compliance reports to the Texas Department of State Health Services (DSHS).

August is structured to support these state-mandated processes by streamlining data entry and documentation. The system allows batch input of screening results and supports high-volume imports, enabling nurses to efficiently record outcomes for large student populations. August also centralizes screening data, referral status, and follow-up activity, improving visibility for Health Services and campuses and reducing the risk of missing state reporting deadlines.

Communicable Disease Reporting

Texas public schools are required to identify, track, and report communicable diseases to the DSHS in accordance with state public health rules. Districts must document confirmed or suspected cases, monitor trends, and submit timely reports when thresholds are met to support outbreak prevention and coordinated public health response.

August includes functionality designed to support these requirements by centralizing communicable disease case entry, documenting symptoms, diagnoses, and exclusion dates, and tracking students' return-to-school clearance. The system provides structured encounter templates that standardize how nurses record illness information and enables Health Services to monitor campus-level trends across the District.

August Electronic Health Records System

In January 2024, Health Services entered a contract with August, a school-focused electronic health records platform designed to streamline student health management. The system went live in August 2024, following the expiration of the previous contract with Frontline. As of December 2025, August includes health information for 136,118 students.

Key functionalities of the August platform include:

- Immunization Compliance: Built-in state-specific immunization rules help assess compliance and identify noncompliant students by age group or vaccine type.
- Medication Administration: Medications taken on a fixed schedule are set up as recurring medications that automatically appear in the system for daily documentation.
- Documentation Tools: Customizable templates and dashboards support efficient and consistent charting.
- System Integration: August integrates with student information systems to enable automatic data syncing.

Roles within the August platform control access to functionality, the ability to manipulate or view information, and access to different documentation templates. The primary purpose of a role is to control the visibility of sensitive information. Each role can be scoped to a given set of students within the District. The role gives access to depth of information, and the student scope gives breadth of information.

There are four different types of roles available in August:

- Sysadmin: Considered super user. Person with access can invite new users, manage other users, add and remove roles, and change the scope of each role. The sysadmin has access to all system capabilities and settings including but not limited to searching for student as well as adding, updating, and deleting student details that may have been inadvertently added by system users. The sysadmin role can reactivate withdrawn students to fulfill documentation request, create and refine templates, add custom medications and create nurse tags.
- Manager: The Manager role is scoped to other users. Managers of other users can see the documentation and activities of their assigned users. The manager role can also invite users and manage users within their scope. However, to access student visit details, the manager needs to also be assigned to another practitioner role (e.g., nurse or clinic aide)
- Nurse: The primary role for school nurses is to document care, administer medications, track immunizations, review health registration information, and manage conditions and allergies. Nurses can open and document treatment sessions for students.

- Clinic Aide: A similar role to nurse including scheduling visits and opening treatment sessions. Nurse assistants are permitted to administer treatment but are not authorized to set up treatment plans or create medical administration schedules (e.g., insulin injection). There are approximately 40 nurse assistants within the District and these assistants are typically assigned to campuses with larger student populations, primarily middle and high schools.

Student Profiles in August

Currently, PowerSchool is the only application interfacing with August, primarily to populate student demographic data. Although August offers a secure family portal that allows parents to access their child's health information, Health Services has opted not to implement this feature due to privacy concerns.

Under Senate Bill (SB) 12, enacted by the 89th Texas Legislature, all school districts are required to obtain annual written parental consent before providing routine physical and mental health services to students. These services include, but are not limited to, first aid, counseling, health screenings, and medication administration. Emergency care is exempt from this requirement. Districts must also notify parents of their rights and any changes to health-related services.

To comply with SB 12, Health Services requires parents to submit the parental consent form through SchoolMint. The consent information is then transmitted to PowerSchool, which now includes a consent-to-treat flag to indicate when a student has a parental consent form on file. August reads this flag and updates the student's profile in the August platform, allowing nurses to easily see that valid parental consent has been provided.

Scope

The audit period included current processes as of fiscal year 2025-2026. Certain other matters or transactions outside that period may have been reviewed to understand and verify information during the audit period.

Objective

The objective of this audit was to assess whether August has implemented effective controls to ensure the accuracy and validity of health data, safeguard data security, and maintain compliance with District policies and applicable regulations.

Methodology

Auditors interviewed key personnel, conducted walkthroughs, and reviewed supporting documents to understand processes and controls surrounding health records management.

Detailed audit procedures are noted below:

1. User Access – To determine whether health data maintained within August Schools is properly restricted, auditors performed the following:
 - Conducted a walkthrough of the login process to verify if Single Sign-On (SSO) or Multi-Factor Authentication (MFA) is required.No observations were noted.

- Reviewed system configurations to confirm the system enforces automatic session logout after 30 minutes of user inactivity.
See Recommendation 1 in this report.
 - Obtained the August user access listing that was provided by Health Services on September 16, 2025, and compared employees and their assigned roles and scopes in August to the active employee listing in Oracle as of September 17, 2025, to verify that they have the appropriate system access based on their titles and locations.
No observations were noted.
 - Reviewed user roles and permissions and conducted a walkthrough to determine whether access levels are appropriately configured in August based on users' job responsibilities.
No observations were noted.
 - Reviewed system audit logs from November 17, 2025, to November 20, 2025, to verify that system access and all recorded data modifications were performed exclusively by authorized users.
No observations were noted.
2. Data Accuracy and Validity – To determine if system controls are in place to ensure the accuracy and validity of data inputs and outputs within August, auditors conducted the following:
- Reviewed system processes to determine if the following automated input controls were implemented, where applicable.
 - Required format field checks (e.g., date, location)
 - Automated field validations (e.g., PowerSchool info pops up)
 - Error messages for invalid entries (e.g., duplicate medication entry)
 - Cross-field checks (e.g., fake student ID detection)
 No observations were noted; however, results were reported to management.
 - Conducted walkthroughs to verify that multiple users can work on the same record or screen simultaneously without data loss.
No observations were noted.
 - Conducted walkthroughs to verify that users can navigate away from a screen to other screens and return without losing previously entered data.
No observations were noted.
3. Regulatory Compliance - To determine if system processes are in place to ensure compliance with federal or state regulations, auditors conducted the following:
- Conducted a walkthrough of School Health and Related Services (SHARS) workflows originating from August through the billing process to verify that process efficiency and accurate documentation are achieved when designing system configurations and data flow. Auditors reviewed for anomalies the August data extract covering services rendered from August 12, 2025, to October 1, 2025.
No observations were noted; however, results were reported to management.
4. Vendor Data Security - To determine whether data is appropriately secured from the vendor's end, auditors conducted the following:

- Obtained and reviewed the vendor's most recent Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to confirm they include documented procedures for restoring services after a disruption.
No observations were noted.
- Obtained and reviewed the vendor's penetration test report released on September 2, 2025, to confirm that penetration testing is performed annually, and findings are remediated post-test.
No observations were noted.
- Obtained and reviewed the vendor's data backup plan and the most recent backup logs to verify that data backup schedule is set up appropriately and backups were performed as stated on the schedule.
No observations were noted.
- Obtained and reviewed the vendor's Incident Response Plan and the three most recent incident reports to confirm that security incidents are handled according to documented procedures and are properly recorded.
See Recommendation 1 in this report.
- Auditors reviewed the award letter between the District and August, Vendor Data Sharing Agreement (DSA), and Service Level Agreement (SLA) to evaluate whether they sufficiently define the vendor's responsibilities for protecting the District data and identify whether they include key terms such as:
 - Data security requirements (e.g., encryption, access controls, MFA)
 - Data privacy and regulatory compliance obligations (e.g., HIPAA)
 - Incident response and breach notification timelines
 - Service availability, uptime, and performance metrics
 - Termination and data return/destruction clauses
 - Vendor reporting and audit rights
 - Scope of services, contract term, and renewal options
 See Recommendation 1 in this report.

Primary criteria used for this audit were:

- 1) National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
- 2) Award Letter RFP RV-207392, January 2024
- 3) DSHS, 2025-2026 Texas Minimum State Vaccine Requirements for Students Grades K-12, Provisional Enrollment, dated February 2025
- 4) Code of Federal Regulations, Title 34 Part 99, Family Educational Rights and Privacy Act (FERPA), October 2025

Audit Observations and Recommendations

Observation 1 – Integration and vendor management of the August system is limited and ineffective.

Condition

August Interfaces for Immunization Data

During enrollment, immunization records provided by parents are uploaded and stored in SchoolMint, which does not electronically interface with August. To populate immunization data in August, the electronic health records system, campus nurses must manually log in to, retrieve, and download information from both SchoolMint and the DSHS' Immunization Registry (ImmTrac2). Thus, populating August with immunization data is a fully manual process at the campus level, primarily by nurses.

Health Services recognized this limitation prior to the audit and is working with EdTech to automate the transfer of immunization records from SchoolMint to PowerSchool, which will then feed into August.

Additionally, August does not interface with ImmTrac2, requiring nurses to manually upload immunization records for state reporting purposes. Although the District submitted all required paperwork for integration, DSHS has not responded since August 2025. Once the ImmTrac2 interface is established, nurses will no longer need to retrieve or upload records manually, reducing the risk of errors and improving centralized tracking.

August Functionality

Auditors reviewed the vendor award letter, service level agreement (SLA), and data sharing agreement to verify that both the vendor and Health Services are adhering to the agreed-upon terms. In addition, system practices were benchmarked against industry best practices (e.g., NIST standards). While the review confirmed general compliance with contractual and operational requirements, several areas for improvement were identified

- The vendor's contract includes a parent portal feature, budgeted at \$42,000 annually. Although Health Services initially planned to use this functionality during the RFP evaluation phase, the feature has not been implemented in either of the first two years of the five-year agreement with annual renewals. Health Services ultimately chose not to enable the portal due to privacy concerns, specifically the risk that parents could inadvertently access other students' sensitive health information, resulting in ongoing costs for functionality that remains unused.
- Users are not automatically logged out after periods of inactivity, despite contract requirements. During testing, auditors remained logged in after 30 minutes of inactivity. Health Services identified this issue prior to report finalization and has already submitted a ticket to the vendor to correct the session timeout configuration.
- The current SLA defines vendor support availability but lacks quantifiable performance metrics such as uptime percentage (e.g., 99.5% monthly availability) or response benchmarks (e.g., ≤3 seconds for data queries).
- Incident response documentation covers external service outages but lacks standardized fields, consistent metrics tracking, and formal processes for documenting mitigations or

lessons learned. Additional refinement is needed to ensure readiness for cybersecurity-related incidents.

Cause

The system integration and vendor management issues stem from limited technical and operational alignment during the procurement, contract negotiation process, and system implementation phases. While Health Services initially considered using the parent portal during the RFP phase, the privacy implications and configuration requirements were not fully evaluated before contract execution. As a result, the implemented solution includes functionality that the department ultimately determined could introduce privacy risks and therefore chose not to enable.

Additionally, certain technical provisions such as measurable system performance metrics (e.g., uptime or response benchmarks consistent with NIST SP 800-53 Rev. 5 SA-9) were not fully defined in the final agreement.

Effect

These issues increase manual workload, create operational inefficiencies, pose additional cost to the district for functionality that is not being used, may limit oversight of vendor performance, and elevate the risk of data errors and unauthorized access.

Recommendation 1

OIA recommends that Health Services strengthen the following activities:

- Continue to work with EdTech to establish the automated interface between SchoolMint and PowerSchool which will feed August.
- Continue to work with the DSHS to establish an automated interface between August and ImmTrac2 to eliminate manual uploads of immunization records.
- Renegotiate the contract prior to the next annual renewal to remove the parent portal feature and exclude the cost for it.
- Configure automatic user logout after a defined period of inactivity and clearly document the timeout duration in the system to meet security requirements
- Consider updating the SLA to include measurable performance indicators such as uptime percentages and system performance benchmarks.
- Consider implementing standardized incident classification and resolution timeframes within August to improve issue tracking and accountability.

Risk Level for Observation 1: Medium¹

¹ See Attachment 1 for Definition of Risk Level.

Conclusion

A reliable and effective electronic health records system is essential for maintaining comprehensive and accurate student health records, enhancing operational readiness, and minimizing the risk of errors, data loss, or resource misuse. Such a system ultimately supports both student safety and districtwide administrative efficiency.

Overall, Health Services has implemented controls to ensure the accuracy and validity of health data, safeguard data security, and maintain compliance with District policies and applicable regulations.

Implementation of the recommendations in this report would assist Health Services enhance the effectiveness and efficiency of its health records management system processes.

We would like to thank the Health Services and SHARS departments for their cooperation and assistance with this audit.

The audit was conducted in conformance with the Institute of Internal Auditors' *Global Internal Audit Standards*. Those standards require OIA to plan and perform the audit to obtain sufficient, reliable, and relevant 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 of Staff and Accountability
Sherry West, Deputy Chief of Staff and Student Services
Jennifer Finley, Executive Director I, Health Services
Marlon Harrison, Chief Technology Officer, Educational Technology Administration
Sean Brinkman, Assistant Superintendent Technology, Enterprise Applications,
Educational Technology Administration

Acknowledgments:

Eva Narten, CPA, CIA, CISA, Deputy Chief, Internal Audit
Richard Siu, CIA, Audit Manager
Claire Chen, CPA, CISA, Auditor II

Definition of Risk Level

Risk Level	Definition
High	These risks could directly impact the achievement of critical strategic or operational objectives of the District. There is a high likelihood of occurrence, and if the event materializes, it could result in a significant negative impact on the District's financial stability, operational efficiency, ability to meet intended outcomes, reputation, or compliance, potentially exceeding the District's risk appetite
Medium	These risks pose a moderate likelihood of occurrence and could have a notable adverse impact on important operational aspects of the District. While undesirable, the potential financial, reputational, strategic or compliance consequences are less severe than high-level risks and may approach the District's risk appetite.
Low	These risks have a low likelihood of occurrence and are expected to have a minimal impact on the District's operational efficiency, financial standing, reputation, or compliance. These risks are generally within the District's risk appetite but still warrant monitoring and may require basic controls.

Management Response

Observation 1 – Integration and vendor management of the August system is limited and ineffective.

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Management Response:

August Interfaces for Immunization Data

- EdTech and the August Implementation Team are actively working on the PowerSchool write-back/feed files project.

Estimated Implementation Date: End of May 2026

Individuals responsible for implementation: Jennifer Finley, Executive Director, Felecia Powell, Data Analyst. Ed Tech Team. With guidance and support from the August Implementation Team (Jake Lerner, Laura Estrada).

- The Texas Department of State Health Services Interoperability Team responded by phone January 22, 2026, to discuss our prior attempts for query only – bi-directional data exchange (IMMTRAC2). On January 29th we received an email with documents to prepare the systems for interface and services.

Estimated Implementation Date: End of July 2026.

Individuals responsible for implementation: Jennifer Finley, Executive Director, Felecia Powell, Data Analyst. August Implementation Team (Jake Lerner, Laura Estrada). Will need guidance from the Texas Department of State Health Services (DSHS) Interoperability Team.

August Functionality

- Renegotiate the contract prior to the next annual renewal to remove the parent portal feature and exclude the cost for it.

Management Response:

This is year two (2) of the contract with electronic health record vendor, August Schools. At least ninety days prior to the third-year renewal period (October 27, 2026), the Executive Director will reach out to the Procurement department to determine next steps to engage the vendor to renegotiate the associated costs of the parent portal feature.

Estimated Implementation Date: October 27, 2026

Individuals responsible for implementation: Jennifer Finley, Executive Director. Will need guidance from the Procurement department.

- Configure automatic user logout after a defined period of inactivity and clearly document the timeout duration in the system to meet security requirements.

Management Response:

Data Analyst, Felecia Powell was given control to set the end inactivity logout time. The chosen inactivity time was 30 minutes. Once an end user becomes inactive, they will be logged out of the system.

Estimated Implementation Date: January 30, 2026

Individuals responsible for implementation: Jennifer Finley, Executive Director, Data Analyst, Felecia Powell. Will need guidance and support from August Implementation Team (Jake Lerner, Laura Estrada).

- Consider updating the SLA to include measurable performance indicators such as uptime percentages and system performance benchmarks.

Management Response:

Management will review the recommendation with the August Team (the vendor) and work collaboratively to establish clear, measurable performance metrics during our bi-weekly calls. Our goal is to define performance metrics that meet our operational needs, that are obtainable within a specified period and allow for review and adjustment. Updates will be provided once discussions with the vendor are complete and proposed metrics are finalized.

Estimated Implementation Date: End of July 2026

Individuals responsible for implementation: Jennifer Finley, Executive Director, Data Analyst, Felecia Powell. Will need guidance and support from August Implementation Team (Jake Lerner, Laura Estrada).

- Consider implementing standardized incident classification and resolution timeframes within August to improve issue tracking and accountability.

Management Response:

Management will review the recommendation with the August Team (the vendor) and strongly encourage the vendor to adopt a standardized incident classification system with defined severity levels and resolution timeframes. This will assist August (the vendor) with issue tracking and strengthen accountability for incident response and resolution.

Estimated Implementation Date: End of July 2026

Individuals responsible for implementation: Jennifer Finley, Executive Director, Data Analyst, Felecia Powell. Will need guidance and support from August Implementation Team (Jake Lerner, Laura Estrada).

Criteria by Observation

Observation 1 – Criteria

Award Letter RFP RV – 207392, January 2024

Health Requirements, page 3

5. IMMTRAC – IMMTRAC interface. Ability to interface with the State immunization database.

NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

SA-9 External System Services, page 271

External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

IR-6 Incident Reporting, page 157

a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period];

Discussion: The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products.

NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

IR-4 Incident Handling, page 152

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

Award Letter RFP RV-207392

Security Administration and Maintenance, page 9

Ability to time-out or suspend users after a period of time of being idle. This time-out requires the user to re-enter their password before continuing.