INTERNAL AUDIT REPORT FOR

Employee Benefits

Gwinnett County Government
Audit Plan Year 2024

December 17, 2024

Gwinnett

GWINNETT COUNTY
INTERNAL AUDIT DIVISION
75 Langley Drive | Lawrenceville, GA 30046
O: 770.822.7757 | F: 770.822.7725
GwinnettCounty.com

Auditors: Jenna Kim, CFE, Senior Auditor
Keenan Nietmann, CFE, Operational Audit Division Director
Leslie Villanueva, CISA, CRISC, IT Audit Division Director

Distribution:

To: Adrienne McAllister, Human Resources Director
Tori Burkholder, Human Resources Deputy Director

CC: Kirkland Carden, Board of Commissioners – District 1, Gwinnett County Audit Committee
Tiana Garner, Clerk of Court, Gwinnett County Audit Committee
Ben Ku, Board of Commissioners – District 2, Gwinnett County Audit Committee Chairman
Glenn Stephens, County Administrator, Gwinnett County Audit Committee
Maria Woods, CPA, Deputy County Administrator/CFO, Gwinnett County Audit Committee

Jonathan Kandel, Deputy County Attorney

This report is intended solely for the individuals contained in the distribution list. Do not send to any other recipients without written authorization.

Table of Contents

Background & Scope 4
Assessment 4
Recommendations 5
Other Considerations 7
Exhibit A: Employee Benefits Disbursements 8
Exhibit B: Summary of Audit Procedures 9

Background & Scope

Gwinnett County (the County) provides comprehensive benefits designed to support employees' health and well-being and safeguard their financial stability. The County's current healthcare benefits include medical, dental, vision, spending accounts, and the County wellness program. County employees working at least 30 hours per week, retirees, the Consolidated Omnibus Budget Reconciliation Act (COBRA) participants, and qualified dependents are eligible for County benefits.

The County's Human Resources Department (HR) is responsible for assisting employees with setting up benefits coverage and making changes during annual enrollment and qualifying life events. HR also approves the County's payments to insurance providers including Aetna, Kaiser, Humana, Cigna, and Voya. For Aetna, the County is self-funded and pays healthcare claims up to a stop-loss limit of $400,000 per participant. The County insures against claims over this threshold through Voya. The County uses AON, an insurance brokerage company, to manage service agreements with insurance providers. During the audit period January 2023 through February 2024, the County paid approximately $106 million to Aetna, Kaiser, Humana, Cigna, and Voya. See **Exhibit A** for net costs by vendor. HR's objectives for employee benefits are as follows:

- Claims and premium payments are accurate, authorized, and only for valid participants.
- Payroll deductions are accurate and complete.
- Activities comply with federal laws and regulations, including Health Insurance Portability and Accountability Act (HIPAA) guidelines.
- Insurance companies adhere to contractual service requirements.

The purpose of this audit was to evaluate the adequacy and effectiveness of management's control activities that are designed to achieve these objectives. Internal Audit (IA) conducted this audit in accordance with the *International Standards for the Professional Practice of Internal Auditing (Standards)*. The Standards require that we plan and perform the audit to identify and evaluate sufficient information to support engagement results. We interviewed employees, observed certain control activities, and reviewed policies and business documents on a sample basis for the audit period. We focused on the County's most significant healthcare benefits costs. We excluded vision insurance and the County wellness program. We believe the evidence provided a reasonable basis for our assessment. See **Exhibit B** for a summary of our audit procedures.

Assessment

We believe management's control activities would benefit from additional structure to provide reasonable assurance of achieving management's key objectives. We tested 14 key controls and included three recommendations to improve claim validation, vendor oversight, and HIPAA training. We found no evidence of abuse or instances of significant improprieties or misuse of funds.

Recommendations

1. Claims validation left to vendors without HR oversight.

The County has a self-funded health benefit plan through Aetna, which means the County is responsible for the cost of claims. Aetna processes and pays healthcare claims and bills the County monthly. AON is a claims administration partner and periodically performs an analysis to identify payments that exceed the $400,000 stop-loss threshold per participant. AON submits the excess payments to Voya for reimbursement to the County. HR receives claims reports from AON and claims data from Aetna regularly. However, HR does not review the details of claims due to the high volume of data. They do not conduct reconciliations before approving the payment for the monthly claims total. Instead, HR relies on AON to validate the claims. According to the County's contract, Aetna provides claims audit services conducted by professional auditors. However, HR reported that they did not receive the audit reports and had no discussions with Aetna regarding audit findings.

RECOMMENDATION

Healthcare providers could potentially charge incorrect amounts or bill for services they did not perform. HR should perform the following control activities to ensure billed services match the care provided for covered employees:

- Review the claims detail reports provided by Aetna and conduct a sample-based review of claims before approving monthly payments to ensure accuracy in processing. This can help HR identify errors, patterns, or recurring issues that could lead to systemic problems.
- Obtain audit results from Aetna and confirm the resolution of any suspicious claims activities identified during the audit.

Management Response

Gwinnett County HR will audit a sample of the Aetna claims data on a monthly basis to ensure those individuals are being processed on the admin invoice correctly. Gwinnett County HR will work with Aetna to obtain their audit results and how discrepancies have been resolved. HR Accounting division will begin the claims audit process in January 2025 and continue monthly.

2. HR unaware of vendor IT security practices or deficiencies.

Sensitive information about the County's plan participants is stored in vendor data systems. If a vendor were to suffer a data breach, the sensitive data may be exposed or misused. Vendors are contractually obligated to notify the County if there is a breach of protected health information (PHI) as required by the HIPAA Breach Notification Rule for Unsecured PHI. However, the contracts do not address how the vendors evaluate their cybersecurity measures for effectiveness. While vendors agree to use appropriate safeguards to prevent the unauthorized use or disclosure of the PHI, the contracts lack details on the safeguards currently in place or planned.

Organizations often review their vendors' System and Organization Controls 2 (SOC 2) reports to evaluate vendors' current risks and controls and ensure control deficiencies are mitigated when applicable. SOC 2 is a compliance framework designed to evaluate and communicate the effectiveness of a vendor's controls in safeguarding customer data. To evaluate HR's process for assessing vendor risks and PHI controls, we inquired about whether HR reviewed the SOC 2 reports or any other relevant documents. HR indicated that they did not obtain SOC 2 reports during the audit period, nor did they review other pertinent documentation.

RECOMMENDATION

Breaches and other security incidents can occur through third parties. HR should regularly evaluate whether vendors manage data with appropriate cybersecurity measures. During the Request for Proposals process, HR should collaborate closely with the Information Technology Services Department (ITS) to review benefits contracts and identify any gaps in cybersecurity protocols. HR should ensure that vendors clearly address their cybersecurity review process in the contracts. To assess the vendors' cybersecurity measures, HR should establish requirements with guidance from ITS, including the regular submission of SOC 2 reports or similar documentation. HR should review these reports regularly to identify any significant deficiencies or changes in vendor operations or security practices.

Management Response

Gwinnett County HR will work with Aon to add cybersecurity measures and requirements in our RFPs moving forward, and that they are considered in the scoring process. We will also partner with all vendors to ensure that we receive and review the latest SOC 2 reports, as well as continuing to monitor how vendors handle sensitive employee data. The timeframe for remediation will be by the end of 2nd quarter in 2025.

3. Required HIPAA training missed or expired for some users.

Organizations handling PHI must comply with HIPAA requirements, including mandatory HIPAA training for employees. Currently, County employees and contractors dealing with PHI are required to complete HIPAA training which covers responsibilities and risks in managing PHI. HR periodically identifies employees who may encounter PHI based on their roles and sends notifications to complete the training. Employees who do not complete the training by the deadline are not supposed to be able to access SAP HCM, which is the employee benefits data module. There are no automated controls to deactivate access for non-compliant accounts. Instead, HR requests ITS to remove the access.

During the audit period, we found that 19 individuals had expired HIPAA training, and upon reviewing the HCM user list, we noted that nine of them (47%) still had access to HCM. Further analysis revealed that out of 231 users on the list, 29 users (13%), including the nine above, had HCM access without the required training. However, HR did not ask ITS to deactivate these users' access. Additionally, HR was unaware of the HIPAA training status of contractors and vendors with HCM access, as there was no process for validating their training or maintaining evidence on file. At the end of fieldwork, we discussed these issues with HR, and HR removed HCM access from users who did not complete the training. These users no longer needed to access the system.

RECOMMENDATION

HIPAA violations can result in penalties. The County should establish written rules and measures for HIPAA training to ensure compliance and avoid potential penalties. HR should outline procedures for individuals who fail to complete the training by the deadline set in HIPAA training guidelines. HR should consider implementing automated controls to deactivate access for non-compliant users and include this in HIPAA training guidelines. Additionally, HR should ensure that all individuals with HCM access, including contractors, stay current on HIPAA training. During periodic reviews of HCM access, HR should verify each user's HIPAA compliance status.

Management Response

We currently have HIPAA training rules established for employees who have access to PHI within the County, however, we do not monitor contractors in a similar manner. Gwinnett County HR will update the current HIPAA training rules and will be sure to include contractors. We will also work closely with our HRIS and IT team to ensure that non-compliant employees' HCM access is removed in a timely manner. We will also work with HRIS to determine which positions within the County no longer need access to PHI and will remove the requirement from their position. Gwinnett County HR expects to complete the remediations for HIPAA by the end of March 2025.

Other Considerations

IA observed opportunities to improve certain business activities based on practices that may, in our opinion, produce good outcomes. The advisory comments are for consideration only, and management is not required to provide written responses or corrective action plans. The advisory comments are as follows:

- To effectively respond to impermissible use or disclosure of PHI, HR should have a written standard that specifies vendor and County roles and responsibilities in following HIPAA requirements. Contracts should cover vendor and subcontractor obligations, including timeframes and procedures for breach notification and response, and provisions to provide free credit monitoring services. There should also be a framework for employees to report suspicious activity or concerns regarding their credit, and procedures for how these reports are handled. In addition to addressing vendor breaches, the standard should outline procedures for breaches of County-housed PHI, including credit monitoring for those affected. The standard should complement ITS incident response standards and focus on HIPAA requirements, coordination with vendors, and communication with affected individuals.
- A CPT code, or Current Procedural Terminology code, is a standardized numerical code used in the medical field to describe medical and diagnostic services and procedures. CPT codes correspond to a specific service or procedure, enabling healthcare providers to clearly communicate services rendered to insurance providers and patients. The County currently operates the Wellness Center for Aetna and Kaiser plan participants to deliver a convenient and cost-effective healthcare experience. The County should consider coordinating with insurance providers to learn the most common CPT codes billed for the County's plan participants. This could help identify opportunities for the County to save money by providing additional services at the Wellness Center when feasible. It could also help identify which current Wellness Center services some employees may not be familiar with.

Exhibit A: Employee Benefits Disbursements

The following chart shows the County's most significant health insurance costs during the audit period, broken down by insurance company. We excluded costs under $3 million per vendor from our review to focus on larger expenditures that significantly contributed to the County's total benefits spending.

Insurance Company	January 2023 Through February 2024
Aetna	$62,026,530
Cigna	5,351,079
Humana	3,177,079
Kaiser	29,909,839
Voya	6,029,879
Total	**$106,494,406**

Data Source: SAP (Unaudited for Financial Reporting Purposes)

Exhibit B: Summary of Audit Procedures

IA performed the following procedures to evaluate the adequacy and effectiveness of control procedures:

- Reviewed County employee benefits policies and procedures for compliance purposes.
- Completed walkthroughs of key benefits administration processes to identify key controls.
- Reconciled (Aetna, Cigna, Humana, Kaiser, and Voya) invoices for the audit period to SAP data to verify the accuracy of the billing records.
- Selected a judgmental sample of three monthly payments made to vendors for January 2023, January 2024, and February 2024 and confirmed HR reconciled and approved the invoices.
- Compared premium rates contained on invoices to the contracts to confirm accuracy.
- Selected a random sample of employees participating in benefit plans and vouched selected employees' payroll withholdings for medical care during the audit period to HR's open enrollment rates without exception. Reviewed sampled employees' dependents and verified their eligibility without exception.
- Assessed the eligibility of all dependents over 26 years old during the audit period for compliance.
- Assessed compliance with COBRA rules and regulations by determining whether all employees terminated during the audit period were notified by HR of COBRA eligibility.
- Sought evidence that billing and collection procedures were in place to ensure the County validated claims and received reimbursements for claims exceeding stop loss thresholds (**Recommendation 1**).
- Obtained the contracts for each healthcare insurance company and confirmed they contained provisions regarding PHI security. Sought evidence that HR confirmed assurance of vendors' implementation of effective controls to protect PHI (**Recommendation 2**).
- Compared a list of employees with the ability to access sensitive healthcare information through SAP HCM to evidence of HIPAA training. Additionally, reviewed the HCM user access report and verified whether each user completed HIPAA training (**Recommendation 3**).
- Interviewed HR and Information Technology staff to obtain an understanding of the employee benefits processes.
- Reviewed the HIPAA Breach Notification Rules and researched vendors' recent data breach cases.