March 2025 | A-04-21-00127

North Carolina's Medicaid Control Environment, Risk Management Practices, and Governing Processes Were Assessed as Moderate Risk

March 2025 | A-04-21-00127

North Carolina's Medicaid Control Environment, Risk Management Practices, and Governing Processes Were Assessed as Moderate Risk

Why OIG Did This Audit

- The OIG has identified improving outcomes in Medicaid as a top management and performance challenge facing the Department of HHS.

- States' management of Medicaid impacts the ability of HHS to effectively manage risk.

- The OIG has previously conducted numerous audits of the North Carolina Medicaid program and reported significant findings in several areas.

- Using an enterprise risk management approach, we assessed North Carolina's control environment, risk management practices, and processes governing its Medicaid program.

What OIG Found

We assessed the risk associated with North Carolina's control environment, risk management practices, and processes governing its Medicaid program as moderate. We found that North Carolina designed and implemented numerous internal controls and risk management practices to administer its Medicaid program. However, for the six risk areas we assessed, we rated three as moderate risk and three as high risk. For the 25 sub-risk areas we assessed, we rated 2 as low risk, 15 as moderate risk, 8 as high risk, and 0 as critical risk.

What OIG Recommends

We recommend that North Carolina develop mitigating controls and strategies to lower risk within the high- and moderate-rated risk areas we identified. We also identified 22 best practices for North Carolina's consideration in taking actions to mitigate risk within high and moderate risk areas.

North Carolina generally agreed with our recommendation and described actions it plans to take in response to the recommendation.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Office of Inspector General (OIG) has identified improving outcomes in Medicaid as a top management and performance challenge facing the Department of Health and Human Services (HHS).[1] Medicaid has been designated as a high-risk program by the Government Accountability Office (GAO) since 2003.[2] Improper payments, oversight of managed care, and program integrity are among areas of concern historically cited by the OIG and GAO. States' management of Medicaid affects the ability of HHS to effectively manage risk.

The OIG has previously conducted numerous audits of the North Carolina Medicaid program and reported significant findings in several areas. (Appendix B lists related OIG reports.)

OBJECTIVE

Our objective was to assess the North Carolina Department of Health and Human Services, Division of Health Benefits' (State agency) control environment, risk management practices, and processes governing its Medicaid program.

BACKGROUND

The Medicaid program provides medical assistance to certain low-income individuals and individuals with disabilities. The Federal and State Governments jointly fund and administer the Medicaid program. At the Federal level, the Centers for Medicare & Medicaid Services (CMS) administers the program. Each State administers its Medicaid program in accordance with a CMS-approved State plan. Although the State has considerable flexibility in designing and operating its Medicaid program, it must comply with applicable Federal requirements. In North Carolina, the State agency administers the Medicaid program.

North Carolina Medicaid Program

In State fiscal year (SFY) 2022 (July 1, 2021, through June 30, 2022), North Carolina's Medicaid program provided services to about 2.9 million recipients at a cost of about $21 billion, with over $14 billion funded by the Federal Government. In July 2021, North Carolina formally began transitioning its Medicaid delivery system from a predominantly fee-for-service model to

---

[1] *2023 Top Management & Performance Challenges Facing HHS*. Accessed on Sep. 16, 2024.

[2] GAO's *High Risk List*. Accessed on Sep. 16, 2024.

managed care.[3] This multi-year transition included transforming business structures and processes, transitioning more than 2 million recipients from fee-for-service to managed care, and managing new managed care health plans—all while maintaining prior fee-for-service business structures and processes for exempt recipients and services not covered by managed care health plans.[4] In 2023, North Carolina signed a bill into law to enable access to care for more than 600,000 residents and provide additional funding to its acute care hospitals.[5] Initial estimates from the State agency projected that the program expansion could result in a combined annual increase of more than $5 billion in Medicaid expenditures.

Guidance for Enterprise Risk Management and Internal Control

Enterprise risk management (ERM) and internal control are components of a governance framework. ERM involves identifying, assessing, and managing risks. Internal control involves processes that provide reasonable assurance that the objectives of an entity will be achieved. Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (the Circular) provides Federal guidance for ERM and internal control, and it describes how they work together to manage risks.[6] The Circular applies to each Federal executive agency, and it has been at the center of Federal requirements to improve accountability in Federal programs and operations. Non-Federal entities are not required to follow the guidance identified in the Circular.

The Circular provides guidance for assessing and improving internal controls based on GAO's *Standards for Internal Control in the Federal Government* (GAO Green Book), which provides a framework for an organization to establish and maintain an effective internal control system. The 2014 GAO Green Book adopted the Committee of Sponsoring Organizations of the

---

[3] Fee-for-service is a method in which healthcare providers are paid for each service performed. Managed care provides health benefits and services through contracted arrangements between State Medicaid agencies and managed care organizations that accept a set per member per month (capitation) payment for these services.

[4] Starting July 1, 2021, most recipients began receiving the same Medicaid services in a new way. Under North Carolina Medicaid Managed Care, recipients choose a health plan and receive care through the health plan's network of doctors. Some excluded or exempt recipients were covered by the State agency's Medicaid Direct fee-for-service program, which also covered some services not covered by managed care health plans.

[5] In March 2023, North Carolina signed House Bill 76 into law (Session Law 2023-7). The bill intended to provide greater access to healthcare options for North Carolina residents by providing increased Medicaid reimbursements to acute care hospitals through the Healthcare Access and Stabilization Program and expanding Medicaid coverage to adults with higher incomes who may not have previously qualified for Medicaid.

[6] In July 2016, OMB updated the Circular to require Federal agencies to implement ERM and better ensure managers were effectively managing risks that could affect achieving strategy and objectives.

Treadway Commission (COSO) 2013 internal control framework principles and adapted them for a government environment.[7, 8]

The Circular also encourages the adoption of an ERM framework, like COSO's *Enterprise Risk Management—Integrating with Strategy and Performance* (June 2017) (COSO ERM), a widely recognized risk management framework. The COSO ERM Framework encompasses internal control with several portions of the text of the original Internal Control Integrated Framework reproduced.[9] Although the guidance identified in the Circular is not required of non-Federal entities, the guidance serves as an effective tool when assessing risk and internal controls.

COSO's ERM framework includes five interrelated components for how management runs an organization. Those components are the following: 1) Governance and Culture; 2) Strategy and Objective-Setting; 3) Performance; 4) Review and Revision; and 5) Information, Communication, and Reporting. The framework further provides a structure for assessing an organization's ERM culture, capabilities, and practices used to manage the risk of not achieving strategy and objectives.

Federal Internal Control Requirements

The Code of Federal Regulations (CFR) requires non-Federal entities to establish and maintain effective internal control, comply with Federal requirements, evaluate and monitor compliance, take prompt action when instances of noncompliance are identified, and safeguard protected personally identifiable and sensitive information (45 CFR § 75.303 "Internal controls"). The regulation states that these internal controls should be in compliance with guidance in the GAO Green Book or the COSO Internal Control Integrated Framework.[10]

---

[7] COSO's *Internal Control - Integrated Framework* (May 2013).

[8] COSO is a joint initiative of private sector organizations dedicated to providing leadership through the development of frameworks and guidance on internal controls, ERM, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.

[9] COSO's *Internal Control - Integrated Framework* was originally issued in 1992.

[10] In its [Frequently Asked Questions](#) document for Uniform Guidance at 2 CFR 200, OMB clarified that similar language under 2 CFR § 200.303(a) does not require federal grant recipients to evaluate internal controls prescriptively in accordance with the GAO Green Book and the COSO Internal Control Integrated Framework. They are provided solely to alert the non-Federal entity to source documents for best practices.

HOW WE CONDUCTED THIS AUDIT

Using an ERM approach based on risk management practices established in COSO's ERM framework and the related GAO Green Book principles, we performed a risk assessment of North Carolina's Medicaid program for SFY 2022. To assess the State agency's control environment, risk management practices, and processes governing its Medicaid program, we identified 6 risk and 25 sub-risk areas using the components of the COSO ERM framework,[11] the GAO Green Book, and the requirements for internal controls under 45 CFR § 75.303.[12] The list below includes each risk area and the sub-risk areas associated with it:

1. **Governance and Culture (5)**—The organization exercises board risk oversight; establishes operating structures; defines desired culture; has a commitment to core values; and attracts, develops, and retains capable staff.

2. **Strategy and Objective-Setting (4)**—The organization analyzes business context, defines risk appetite, evaluates alternative strategies, and formulates business objectives.

3. **Performance (5)**—The organization identifies risk, assesses the severity of risk, prioritizes risks, implements risk responses, and develops a portfolio view of risk.

4. **Review and Revision (3)**—The organization assesses substantial change, reviews risk and performance, and pursues improvement in ERM.

5. **Information, Communication, and Reporting (3)**—The organization leverages information and technology; communicates risk information; and reports on risk, culture, and performance.

6. **Federal Internal Control Requirements (5)**—The organization adopts an internal control framework, implements controls over compliance, evaluates and monitors its compliance, resolves findings of noncompliance, and safeguards sensitive information.

We developed questionnaires to gather data from the State agency, evaluated the State agency's written responses, reviewed its supporting documentation, and interviewed State agency management. We then determined a risk level (low, moderate, high, or critical) for each risk and sub-risk area and used this information to assess the overall risk associated with the State agency's control environment, risk management practices, and processes governing its Medicaid program.

---

[11] Within the 5 components of the COSO ERM framework, 20 risk management principles represent the fundamental concepts associated with each component. These principles represent steps an organization would take as part of its ERM practices.

[12] 45 CFR § 75.303 lists five internal control requirements for non-Federal entities. These requirements are referred to in this report as "Federal Internal Control Requirements." We assessed the Federal Internal Control Requirements under 45 CFR § 75.303 and considered the subsections under 45 CFR § 75.303 as five sub-risk areas.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

Appendix A contains our scope and methodology.

RESULTS OF AUDIT

Overall, we assessed the risk associated with the State agency's control environment, risk management practices, and processes governing its Medicaid program as moderate.[13] We found that the State agency designed and implemented numerous internal controls and risk management practices to administer its Medicaid program. However, for the six risk areas we assessed, we rated three as moderate risk and three as high risk. For the 25 sub-risk areas we assessed, we rated 2 as low risk, 15 as moderate risk, 8 as high risk, and 0 as critical risk (see table below and a complete risk assessment in Appendix D).

Table 1: Risk Levels

NC Medicaid Risk and Sub-Risk Areas
Moderate: Governance and Culture
Sub-Risks: 🟢 2 Low   🟡 2 Moderate   🔴 1 High
High: Strategy and Objective-Setting
Sub-Risks: 🟡 2 Moderate   🔴 2 High
Moderate: Performance
Sub-Risks: 🟡 5 Moderate
High: Review and Revision
Sub-Risks: 🟡 1 Moderate   🔴 2 High
Moderate: Information, Communication, and Reporting
Sub-Risks: 🟡 3 Moderate
High: Federal Internal Control Requirements
Sub-Risks: 🟡 2 Moderate   🔴 3 High

🟡 **GOVERNANCE AND CULTURE**

We rated the Governance and Culture risk area as moderate risk. According to risk management practices,[14] governance sets the organization's tone, reinforcing the importance

---

[13] We used the average risk rating for each risk and sub-risk area to calculate a numeric entity rating and to assess overall risk using the heat map in Appendix C.

[14] The risk management practices refer to those established in COSO's ERM framework and the related GAO Green Book principles.

of and establishing oversight responsibilities for ERM. Culture pertains to ethical values, desired behaviors, and understanding risk within the entity. Of the five sub-risk areas within Governance and Culture, we rated two (*Defines Desired Culture* and *Demonstrates Commitment to Core Values*) as low risk, two (*Exercises Board Risk Oversight* and *Establishes Operating Structures*) as moderate risk, and one (*Attracts, Develops, and Retains Capable Individuals*) as high risk.

The State agency established an oversight board, the executive team, which met regularly. In addition, it established multiple committees that reported to the executive team and enhanced governance and risk management. The State agency had a defined organizational structure, which it revised and updated for the transformation of its Medicaid program to managed care. The State agency has also taken recent actions to improve its culture related to risk management, such as establishing forums for discussing risk and implementing new ERM practices. Also, in early 2023, new leadership at the State agency communicated priorities, staffing changes, and plans to foster ERM, and it collaborated with OIG throughout this risk assessment.

We rated *Defines Desired Culture* and *Demonstrates Commitment to Core Values* sub-risk areas as low risk because the State agency defined and communicated expectations on its core values and standards of conduct. [15] It also had controls to enforce accountability to core values, like employee performance evaluation standards aligned with core values. However, we rated *Exercises Board Risk Oversight* and *Establishes Operating Structures* sub-risk areas as moderate risk because, among other things, the State agency's policies and procedures did not:

- define the requirements for oversight board members, including their entity knowledge, relevant expertise, the number of members, specialized skills required, and possible independence needed to fulfill oversight responsibilities;

- provide for periodic assessments of its operating structure and reporting lines;

- define factors to be considered when evaluating and modifying its operating structures; and

- have controls for defining roles, authorities, and responsibilities of operating units, teams, and functions.

In addition, we rated the *Attracts, Develops, and Retains Capable Individuals* sub-risk area as high risk because, among other things, the State agency:

---

[15] The State agency used core values established by its higher command, the North Carolina Department of Health and Human Services (NCDHHS). These core values included Belonging, Joy, People-Focused, Proactive Communication, Stewardship, Teamwork, and Transparency.

- lacked formal succession and contingency plans, controls for assessing and managing excessive pressures on staff, mechanisms to reward and motivate staff performance, and formal recruitment, training, and mentoring plans; and
- had concerns about attracting and retaining staff at the State and County levels, staff burnout, high turnover, inability to obtain permanent positions, and lack of business continuity.

Without improving its controls related to governance, the State agency may exercise oversight with a body that does not have the appropriate composition, collective competencies, or objectivity to carry out its governance responsibilities, and it may not adapt its operating structures and delegate responsibilities to effectively pursue new objectives, such as new laws or regulations. Collectively, failure to address risks related to human capital could have long-term negative effects on the program.

⬤ STRATEGY AND OBJECTIVE-SETTING

We rated the Strategy and Objective-Setting risk area as high risk. According to risk management practices, ERM, strategy, and objective-setting work together in the strategic planning process. Business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk. Of the four sub-risk areas within Strategy and Objective-Setting, we rated two (*Analyzes Business Context* and *Defines Risk Appetite*) as moderate risk and two (*Evaluates Alternative Strategies* and *Formulates Business Objectives*) as high risk.

The State agency implemented various controls to analyze business context, including governance committees with responsibilities for considering internal and external environmental factors. It identified strategy sessions and other leadership meetings that it held for Medicaid planning. The State agency was also drafting procedures for formally establishing goals and objectives and considering performance measures. However, we rated *Analyzes Business Context* and *Defines Risk Appetite*[16] sub-risk areas as moderate risks because, among other things, the State agency did not:

- provide any assessments or evaluations of its external environment for its strategic planning and did not establish formal procedures to govern such assessments; and

- formally define its risk appetite or establish related procedures.

Additionally, we rated *Evaluates Alternative Strategies* and *Formulates Business Objectives* sub-risk areas as high risk because, among other things, the State agency:

---

[16] Risk appetite is generally the types and amount of risk, on a broad level, an organization is willing to accept.

- lacked formal policies and procedures to govern its strategic planning and evaluation of alternative strategies, did not provide strategic plans, and did not provide data and analysis used in recent strategic planning; and

- did not document its objectives or establish formal performance measures to assess achieving objectives.

Formal procedures to govern the assessment of the external environment could increase the likelihood that the State agency considers external political, economic, social, technological, legal, and environmental factors that could affect achieving objectives. Also, because it did not define its risk appetite, decision-making at varying levels of the organization may be inconsistent with the types and amount of risk it is willing to accept. The lack of formal policies and procedures for planning and evaluating alternative strategies could lead to missed opportunities, increased costs, inefficient resource allocation, and overlooking potential risks. The absence of defined business objectives may contribute to a lack of accountability for performance, difficulty in measuring success, and increased risk of failing to achieve strategy.

⬤ PERFORMANCE

We rated the Performance risk area as moderate risk. According to risk management practices, Performance includes identifying and assessing risks that may affect an entity's ability to achieve strategy and business objectives. Risks should be prioritized by severity in the context of risk appetite. The organization then selects risk responses and considers all the risk it has assumed. We rated all five (*Identifies Risk, Assesses Severity of Risk, Prioritizes Risks, Implements Risk Responses,* and *Develops Portfolio View*) sub-risk areas within Performance as moderate risk.

The State agency's organizational structure included cross-functional committees that facilitated identifying and assessing risks at multiple levels and reporting risks to the executive team. In support of its program transformation to managed care, it deployed formal processes and procedures for identifying, assessing, mitigating, and monitoring risks and issues across the organization.[17] The State agency acknowledged these transformation risk management practices were effective at identifying and mitigating risks and indicated it would evaluate the continued effectiveness of these procedures as it approached completion of its transformation.

The State agency assessed risk severity to varying degrees and had a process to respond to identified risks. Furthermore, its Office of Compliance and Program Integrity (OCPI) had a planned Compliance Monitoring Program that included embedded risk identification procedures to evaluate internal compliance and risk mitigation across all Medicaid operational areas. However, we rated *Identifies Risk, Assesses Severity of Risk, Prioritizes Risks, Implements*

---

[17] Processes and procedures included the North Carolina Medicaid Transformation Program Risk and Issue Management Plan and associated tools, logs, and meetings.

Risk Responses, and *Develops Portfolio View* sub-risk areas as moderate risk because, among other things, the State agency:

- had not fully implemented its newly planned OCPI Compliance Monitoring Program, which included internal risk assessments;

- assessed severity of risks without fully considering inherent risk, residual risk, or the relative severity of each of the risks to achieving a given strategy or business objective;

- assigned risks a severity rating, but it did not address how to prioritize risks with similar ratings;[18]

- did not have formal procedures to define, select, and consider the costs and benefits of different risk responses; and

- did not deploy complex or advanced procedures to evaluate its risks in the context of all risks it faces instead of individual risks in isolation.[19]

OCPI's Compliance Monitoring Program should improve the State agency's risk identification capability. Improving procedures for assessing severity could also help the State agency better estimate or understand the significance of risks affecting achieving strategy and objectives. Improving its prioritization of risks may facilitate more effective evaluations of the trade-offs between allocating resources to mitigate one risk versus another. Implementing formal risk responses may help the State agency better consider the costs and benefits of potential responses to identified risks. Also, by improving its procedures for evaluating a portfolio view of risk, the State agency may better consider the interdependencies of its risks and how certain risks collectively affect performance.

● REVIEW AND REVISION

We rated the Review and Revision risk area as high risk. According to risk management practices, by reviewing its performance the organization considers how well the ERM components function over time and what revisions are needed as changes occur. Of the three sub-risk areas within Review and Revision, we rated one (*Assesses Substantial Change*) as moderate risk and two (*Reviews Risk and Performance* and *Pursues Improvement in ERM*) as high risk.

---

[18] COSO ERM guidance provides examples of factors to consider, such as adaptability, complexity, velocity, persistence, and recovery, when prioritizing risks.

[19] A portfolio view allows management to consider the type, severity, and interdependencies of risks and how they may affect performance.

With its transition to managed care, the State agency used meetings and dashboards to track the status and completion of focused operational efforts. The State agency also adopted several new risk management practices and made some organizational changes that enhanced its risk management. However, we rated *Assesses Substantial Change* sub-risk area as moderate risk because, among other things, the State agency did not have a formal strategy and policy for identifying and assessing substantial changes to its internal and external environment.

In addition, we rated *Reviews Risk and Performance* and *Pursues Improvement in ERM* sub-risk areas as high risk because, among other things, the State agency did not have:

- a formal policy for managing internal assessments of performance or for reviewing performance measures relative to achieving strategy and business objectives; and

- a formal documented ERM strategy or policies governing its collective risk management practices.

Without a formal policy for assessing substantial changes, the State agency may not respond timely to some internal and external changes that could significantly affect its ability to achieve objectives. Without a formal policy for assessing its performance, the State agency's efforts to identify areas of improvement, implement necessary changes, and enhance overall performance may be degraded. A more deliberate ERM strategy should improve the State agency's risk management practices and improve its ability to identify, assess, and manage the complex risks facing its Medicaid program.

🟡 INFORMATION, COMMUNICATION, AND REPORTING

We rated the Information, Communication, and Reporting risk area as moderate risk. According to risk management practices, an organization should have a continual process for obtaining and sharing necessary information from both internal and external sources across the organization. We rated all three (*Leverages Information and Technology, Communicates Risk Information,* and *Reports on Risk, Culture, and Performance*) sub-risk areas within the Information, Communication, and Reporting risk area as moderate risk.

The State agency used its information systems to collect and use information for decision-making, and it had some controls for managing its internal and external reporting. However, we rated *Leverages Information and Technology, Communicates Risk Information,* and *Reports on Risk, Culture, and Performance* sub-risk areas as moderate risk because, among other things, the State agency did not:

- provide documentation of reliability testing of data used for decision-making;

- provide formal policies governing its communication with internal and external stakeholders, whistle-blower programs, ethics hotlines, and similar programs; and

- identify all regulatory reporting requirements and internal and external report users.

Without additional controls, the State agency may not effectively define its reporting objectives and has an increased risk that it will not meet some regulatory reporting requirements. Management decisions could also be based on inaccurate, incomplete, or biased data.

● FEDERAL INTERNAL CONTROL REQUIREMENTS

Federal regulations require non-Federal entities, like State Medicaid agencies, to establish and maintain effective internal control over Federal awards. According to 45 CFR § 75.303 "Internal controls," non-Federal entities must:

(a) Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government," issued by the Comptroller General of the United States, or the "Internal Control Integrated Framework," issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

(b) Comply with Federal statutes, regulations, and the terms and conditions of the Federal awards.

(c) Evaluate and monitor the non-Federal entity's compliance with statutes, regulations and the terms and conditions of Federal awards.

(d) Take prompt action when instances of noncompliance are identified including noncompliance identified in audit findings.

(e) Take reasonable measures to safeguard protected personally identifiable information and other information the HHS awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.

We assessed the Federal Internal Control Requirements under 45 CFR § 75.303 and considered the subsections under 45 CFR § 75.303 as five sub-risk areas. We rated the Federal Internal Control Requirements risk area as high risk. Of the five sub-risk areas, we rated two (*Resolves Findings of Noncompliance* and *Safeguards Sensitive Information*) as moderate risk and three

(*Adopts an Internal Control Framework, Implements Controls Over Compliance,* and *Evaluates and Monitors Compliance*) as high risk.

The State agency established certain organizational oversight structures, internal risk management practices, and various operational-level procedures over compliance and monitoring compliance. For example, its OCPI provided some internal compliance oversight. In addition, the North Carolina Department of Health and Human Services (NCDHHS) Office of Internal Audit (OIA) performed some Medicaid audits and internal control assessments through the Enhancing Accountability in Government through Leadership and Education (EAGLE) program.[20] Furthermore, external auditors with the State of North Carolina also performed an annual Statewide Single Audit.[21] The State agency indicated that they have implemented corrective action plans for addressing audit findings and followed NCDHHS policies and procedures for safeguarding information and performed related training of staff. However, we rated *Resolves Findings of Noncompliance* and *Safeguards Sensitive Information* sub-risk areas as moderate risk because, among other things, the State agency:

- lacked policy governing how it manages and resolves findings of noncompliance and had some weakness in procedures for identifying, evaluating, and resolving internally identified control deficiencies; and

- did not perform internal reviews or assessments of the procedures it implemented to safeguard personally identifiable information and other sensitive information.

In addition, we rated the *Adopts an Internal Control Framework, Implements Controls Over Compliance,* and *Evaluates and Monitors Compliance* sub-risk areas as high risk because, among other things, the State agency did not:

- adopt an internal control framework and generally did not use internal control standards, like the standards identified within the GAO Green Book or COSO's internal control framework, to establish and maintain its internal controls;

---

[20] The North Carolina Office of State Controller initiated the EAGLE program with the intent of assisting agencies with identifying risks and compensating controls that reduce the possibility of material misstatements, misappropriation of assets, and noncompliance with rules and regulations. We considered the results from prior EAGLE assessments in performing our risk assessment.

[21] As required for Federal awards under 2 CFR § 200, the North Carolina Office of the State Auditor performs an annual Statewide Single Audit, formerly known as an A-133 Audit. This audit is an organization-wide financial statement and Federal awards audit of non-Federal entities, like the State of North Carolina, which expend $750,000 or more in Federal funds in 1 year. The Single Audits are intended to provide some assurance to the Federal Government that a non-Federal entity has adequate internal controls in place and is generally in compliance with program requirements. We considered the results from prior Single Audit reports in performing our risk assessment. See Single Audit | HHS.gov.

- fully or formally document entity-level policies or strategic plans governing the design and implementation of its controls over compliance; and

- fully develop and document policies governing the design and implementation of internal controls for monitoring compliance.

Strengthening policies and procedures for resolving noncompliance could improve the State agency's ability to respond to and remediate deficiencies and related compliance risks. In addition, without evaluating its controls for protecting sensitive information, the State agency lacks some assurance against unauthorized access, use, or disclosure of personally identifiable information that could harm individuals by contributing to potential identity theft and harm the State agency by reducing public trust. The deployment of an internal control framework and standards is foundational to establishing and maintaining a strong internal control system. Entity-level policies or strategic plans over compliance could further improve the State agency's control environment. Additionally, similar controls over monitoring compliance could reduce the risk of not achieving compliance objectives.

CONCLUSION

Within 6 risk areas, we identified 25 sub-risk areas, rating 2 as low, 15 as moderate, 8 as high, and 0 as critical risk. Overall, we assessed the risk associated with the State agency's control environment, risk management practices, and processes governing its Medicaid program as moderate risk. The program was rated moderate risk because these risk levels indicate that, although the State agency has developed and implemented some controls, it may not effectively identify, assess, and manage some risks, and its internal controls may not effectively prevent and detect some noncompliance with Federal requirements.

RECOMMENDATION

We recommend that the North Carolina Department of Health and Human Services, Division of Health Benefits develop mitigating controls and strategies to lower risk within the high- and moderate-rated risk areas we identified.

We also identified 22 best practices in Appendix E for the State agency's consideration when taking actions to mitigate risk within high and moderate risk areas.

STATE AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

STATE AGENCY COMMENTS

In written comments on our draft report, the State agency generally agreed with our recommendation. The State agency indicated that some specific risks identified in the report appeared less applicable to a State government agency and more suited for a private enterprise. However, it agreed with the intent and goal of the review and fully supported the approach to facilitate a collaborative exchange with CMS. The State agency identified plans to pursue additional strategies to enhance its oversight and lower risk including pursuit of a formal enterprise risk management program and associated investments in new staff roles, education and training, policy development, and technology solutions for tracking and reporting.

The State agency's comments are included in their entirety as Appendix F.

OFFICE OF INSPECTOR GENERAL RESPONSE

We commend the State agency for taking or considering corrective action, although we have not formally reviewed those actions.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We performed a risk assessment of the State agency for SFY 2022 (July 1, 2021, through June 30, 2022), which aligned with the launching of managed care in North Carolina, and considered recent data relative to the State agency's transformation. The OIG initially announced two projects to separately conduct risk assessments of the managed care (A-04-21-09004) and the fee-for-service components (A-04-21-00127) of the program. However, because of significant overlap and duplication, we consolidated these risk assessments into this report.

To assess the State agency's control environment, risk management practices, and processes governing its Medicaid program, we identified 6 risk and 25 sub-risk areas using the components of the COSO ERM framework, the GAO Green Book, and the requirements for internal controls under 45 CFR § 75.303. We assessed each sub-risk area by reviewing documents and evaluating written responses obtained from the State agency, considering risk factors, assigning a numerical risk rating to the risk factors, and calculating a numeric risk rating for each risk factor considered.[22] We then averaged the numeric risk rating of all factors considered to determine the numeric risk rating for each sub-risk area. We averaged each risk area's sub-risk area risk ratings to calculate the numeric risk rating for the risk area and to determine risk levels using the heat map in Appendix C.[23] Using this information, we assessed the overall risk associated with the State agency's control environment, risk management practices, and processes governing its Medicaid program.

We did not test any transactions or the effectiveness of internal controls in performing this risk assessment.

METHODOLOGY

To accomplish our objective, we took the following steps:

- reviewed applicable Federal laws, policies, and guidance;

- requested information and evaluated written responses from management and oversight partners, including CMS, the State auditor, and the NCDHHS OIA, regarding the State agency's risk management practices, internal controls, and risks;

---

[22] We assessed whether the COSO ERM principles, the GAO Green Book principles, and the standards derived from 45 CFR § 75.303 "Internal Controls" were present and functioning, and we considered the maturity of related risk management practices and internal controls. We also considered likelihood of occurrence and severity of impact in calculating the numeric risk rating for each factor.

[23] To determine risk levels, we rounded risk ratings as follows: 1 to less than 4.5 (Low); 4.5 to less than 8.5 (Moderate); 8.5 to less than 14.5 (High); and 14.5 and greater (Critical).

- reviewed prior reports from the OIG, State auditor, and OIA;

- developed risk assessment questionnaires for the enterprise level and specific operational units and functions, including recipients' eligibility, provider enrollment, provider payments, data and information systems, contract monitoring, and financial management;

- evaluated the State agency's written responses to our questionnaires and analyzed them in the context of the COSO ERM framework, GAO Green Book, and Federal Internal Control Requirements;

- held discussions with the State agency about the program, certain processes, and risks;

- determined a risk level for each risk and sub-risk area;

- used the risk level for each risk and sub-risk area to assess the overall risk associated with the State agency's control environment, risk management practices, and processes governing its Medicaid program;

- assessed mitigating processes and strategies for identified risks; and

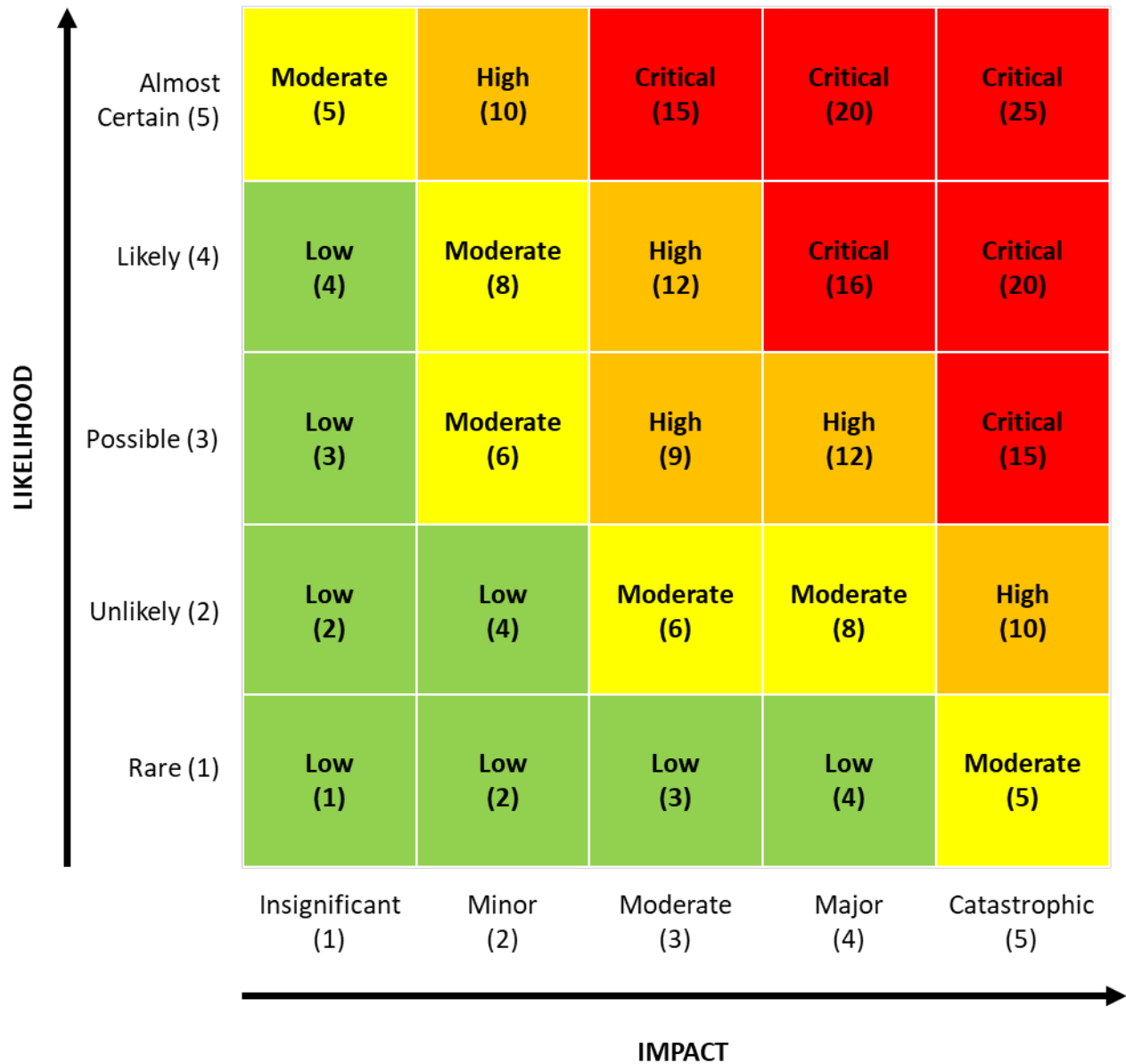- discussed the results with State agency officials.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

APPENDIX B: RELATED OFFICE OF INSPECTOR GENERAL REPORTS

Report Title	Report Number	Date Issued
North Carolina Did Not Report and Return All Medicaid Overpayments for the State's Medicaid Fraud Control Unit Cases	A-06-23-04004	6/20/2024
North Carolina Did Not Always Invoice Rebates to Manufacturers for Physician-Administered Drugs	A-07-21-07002	2/7/2023
North Carolina Made Capitation Payments to Managed Care Entities After Beneficiaries' Deaths	A-04-16-00112	9/25/2020
North Carolina Should Improve its Oversight of Selected Nursing Homes' Compliance With Federal Requirements for Life Safety and Emergency Preparedness	A-04-19-08070	9/18/2020
North Carolina Did Not Ensure That Nursing Facilities Always Reported Allegations of Potential Abuse and Neglect of Medicaid Beneficiaries and Did Not Always Prioritize Allegations Timely	A-04-17-04063	7/29/2020
North Carolina Received $30 Million in Excess Federal Funds Related to Improperly Claimed Health Home Expenditures	A-04-18-00120	4/29/2020
North Carolina Did Not Always Verify Correction of Deficiencies Identified During Surveys of Nursing Homes Participating in Medicare and Medicaid	A-04-17-02500	1/4/2018
The State of North Carolina Did Not Meet Federal Information System Security Requirements for Safeguarding Its Medicaid Eligibility Determination Systems and Data	A-07-16-00486	12/7/2017
North Carolina Did Not Comply With Federal and State Requirements When Making Medicaid Cost-Sharing Payments for Professional Medical Services	A-04-16-04054	11/7/2017
Public Summary Report: The State of North Carolina Did Not Ensure That Federal Information System Security Requirements Were Met for Safeguarding Its Medicaid Claims Processing Systems and Data	A-07-16-00469	8/16/2017
North Carolina Improperly Claimed Federal Reimbursement for Some Medicaid Nonemergency Transportation Services	A-04-15-04037	11/18/2016
North Carolina Claimed Millions in Unallowable School-Based Medicaid Administrative Costs	A-04-15-00101	10/6/2016
North Carolina Did Not Always Make Correct Medicaid Claim Adjustments	A-04-14-00100	3/24/2016
North Carolina Received Millions in Unallowable Bonus Payments	A-04-14-08035	7/21/2015
North Carolina Claimed Federal Medicaid Reimbursement for Dental Services That Did Not Always Comply With Federal and State Requirements	A-04-13-04014	3/26/2015

APPENDIX C: HEAT MAP FOR DETERMINING RISK LEVELS

We used this heat map to assess a risk level (low, moderate, high, or critical) for each sub-risk area, risk area, and overall risk.[24]

LIKELIHOOD	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	Moderate (5)	High (10)	Critical (15)	Critical (20)	Critical (25)
Likely (4)	Low (4)	Moderate (8)	High (12)	Critical (16)	Critical (20)
Possible (3)	Low (3)	Moderate (6)	High (9)	High (12)	Critical (15)
Unlikely (2)	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
Rare (1)	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)

IMPACT

---

[24] To calculate the numeric risk rating in each box, the likelihood of occurrence is multiplied by the severity of impact. For example, the likelihood of "Possible (3)" and the impact of "Minor (2)" would result in "Moderate (6)" (3 x 2 = 6). To determine risk levels, we rounded risk ratings as follows: 1 to less than 4.5 (Low); 4.5 to less than 8.5 (Moderate); 8.5 to less than 14.5 (High); and 14.5 and greater (Critical).

APPENDIX D: COMPLETE RISK ASSESSMENT

RISK

SUB-RISK

🟡 Governance and Culture	🔴 Strategy and Objective-Setting	🟡 Performance	🔴 Review and Revision	🟡 Information, Communication, and Reporting	🔴 Federal Internal Control Requirements
🟡 Exercises Board Risk Oversight	🟡 Analyzes Business Context	🟡 Identifies Risk	🟡 Assesses Substantial Change	🟡 Leverages Information and Technology	🔴 Adopts an Internal Control Framework
🟡 Establishes Operating Structures	🟡 Defines Risk Appetite	🟡 Assesses Severity of Risk	🔴 Reviews Risk and Performance	🟡 Communicates Risk Information	🔴 Implements Controls Over Compliance
🟢 Defines Desired Culture	🔴 Evaluates Alternative Strategies	🟡 Prioritizes Risk	🔴 Pursues Improvement in Enterprise Risk Management	🟡 Reports on Risk, Culture, and Performance	🔴 Evaluates and Monitors Compliance
🟢 Demonstrates Commitment to Core Values	🔴 Formulates Business Objectives	🟡 Implements Risk Responses			🟡 Resolves Findings of Noncompliance
🔴 Attracts, Develops, and Retains Capable Individuals		🟡 Develops Portfolio View			🟡 Safeguards Sensitive Information

RISK LEVELS

🟢 LOW   🟡 MODERATE   🟠 HIGH   🔴 CRITICAL

APPENDIX E: BEST PRACTICES FOR RISK MITIGATION

Table 2 contains best practices for the State agency's consideration in developing, implementing, and improving risk management practices and internal controls to mitigate risks within the high- and moderate-rated risk areas. The table identifies 22 best practices and the associated risk area, sub-risk area(s), GAO Green Book internal control principles, and risk level. We have ordered these by numeric risk rating from high to moderate with the highest listed first.

Table 2: Best Practices for Risk Mitigation

| #	Best Practices	Risk Area	Sub-Risk Area(s)	GAO Green Book	Risk Level
1	Perform a detailed assessment, develop a strategy, and coordinate and engage with the State Legislature, as necessary, to mitigate staffing and human capital risks.	Governance and Culture	Attracts, Develops, and Retains Capable Individuals	GAO Principle 10	🟠
2	Develop and implement plans, policies, procedures, and controls for recruitment, training, mentoring, performance incentives, succession plans, contingency plans, and addressing excessive pressures on staff.	Governance and Culture	Attracts, Develops, and Retains Capable Individuals	GAO Principles 4 and 5	🟠
3	Establish formal business objectives in specific and measurable terms.	Strategy and Objective-Setting	Formulates Business Objectives	GAO Overview Section 2; GAO Principle 6	🟠
4	Implement formal policies, procedures, and controls to guide strategic planning.	Strategy and Objective-Setting	Evaluates Alternative Strategies	GAO Overview Section 2; GAO Principle 6	🟠
5	Implement formal policy-managing internal assessments of performance against performance measures.	Review and Revision	Reviews Risk and Performance	GAO Principles 6 and 10	🟠

6	Develop an ERM strategy and evaluate the cost-benefit of adopting and integrating a formal ERM program.	Review and Revision	Pursues Improvement in ERM	N/A	🔴
7	Formally adopt an internal control framework and use recognized internal control standards to enhance efforts to establish and maintain effective internal controls over the Federal award.	Federal Internal Control Requirements	Adopts an Internal Control Framework	GAO Principle 3	🔴
8	Fully and formally develop and implement policies and strategic plans for the design and implementation of controls over compliance.	Federal Internal Control Requirements	Implements Controls over Compliance	GAO Principle 10	🔴
9	Fully develop and implement policies and plans for the design and implementation of internal controls for monitoring compliance.	Federal Internal Control Requirements	Evaluates and Monitors Compliance	GAO Principle 16	🔴
10	Develop additional procedures for considering the costs and benefits of risk responses.	Performance	Implements Risk Responses	GAO Principles 7 and 10	🟡
11	Evaluate how implementing a risk appetite could improve strategic planning and objective-setting.	Strategy and Objective-Setting	Defines Risk Appetite	N/A	🟡
12	Provide additional leadership direction on internal risk identification, assessment, and management tools.	Performance	Identifies Risk	GAO Principle 7	🟡
13	Develop additional controls for assessing the severity of risk, prioritizing risks, and developing and analyzing a portfolio view of risks that effect strategy and objectives.	Performance	Assesses Severity of Risk, Prioritizes Risks, Develops Portfolio View	GAO Principle 7	🟡
14	Develop formal policy governing communication with internal and external stakeholders.	Information, Communication, and Reporting	Communicates Risk Information	GAO Principles 14 and 15	🟡

15	Develop additional controls guiding the oversight board and define the knowledge, relevant expertise, number of members, and possible independence needed to fulfill oversight responsibilities.	Governance and Culture	Exercises Board Risk Oversight	GAO Principle 2	🟡
16	Implement formal policies and procedures for analyzing external factors and risks when developing strategy and objectives.	Strategy and Objective-Setting	Analyzes Business Context	GAO Principles 6 and 7	🟡
17	Develop strategy and implement a formal policy for identifying and assessing substantial changes and associated risks.	Review and Revision	Assesses Substantial Change	GAO Principle 9	🟡
18	Assess internal and external reporting, define reporting objectives, and ensure all regulatory reporting requirements are defined.	Information, Communication, and Reporting	Reports on Risk, Culture, and Performance	GAO Overview Section 2; GAO Principles 14 and 15	🟡
19	Develop formal policy for managing the resolution of noncompliance and strengthen internal procedures for identification, evaluation, and resolution of internal control deficiencies.	Federal Internal Control Requirements	Resolves Findings of Noncompliance	GAO Principle 17	🟡
20	Develop and implement policies and procedures for assessing controls over safeguarding information.	Federal Internal Control Requirements	Safeguards Sensitive Information	GAO Principle 11	🟡
21	Develop and implement formal policies and controls for periodically assessing operating structures and for defining roles, authorities, and responsibilities of operating units, teams, and functions.	Governance and Culture	Establishes Operating Structures	GAO Principle 3	🟡
22	Document procedures for reliability testing of data used for decision-making.	Information, Communication, and Reporting	Leverages Information and Technology	GAO Principle 13	🟡

Docusign Envelope ID: 138942290-A4F0-4A61-853D-23484890672F
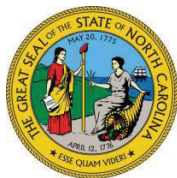
NC DEPARTMENT OF
HEALTH AND
HUMAN SERVICES
Division of Health Benefits

ROY COOPER • Governor
KODY H. KINSLEY • Secretary
JAY LUDLAM • Deputy Secretary, NC Medicaid

December 16, 2024

Truman Mayfield
Regional Inspector General for Audit Services
Office Of Audit Services, Region IV
61 Forsyth Street, SW, Suite 3T41
Atlanta, GA 30303

Re: Report Number: A-04-21-00127

Dear Mr. Mayfield:

We have reviewed your draft report *North Carolina's Medicaid Control Environment, Risk Management Practices, and Governing Processes Were Assessed as Moderate Risk* (Report) covering the audit period July 1, 2021, through June 30, 2022. The NC Department of Health and Human Services, Division of Health Benefits ("Department") appreciates the efforts undertaken to produce this report and the insight it provides in relation to the practices in place during the review period. The Department fully acknowledges its responsibility to assess and mitigate risks to the Medicaid program and continues to invest time and talent in reviewing and enhancing its operations. In the 2 years since the review period closed, the Department continued to invest and evolve our governance and oversight models to protect the well-being of the people who rely on NC Medicaid, while protecting the integrity of the program. The Department further appreciates the acknowledgement of the successfully established practices and processes as called out in the report. The following represents our response to the recommendation.

RECOMMENDATION: **DEVELOP MITIGATING CONTROLS AND STRATEGIES TO LOWER RISK WITHIN THE HIGH- AND MODERATE-RATED RISK AREAS IDENTIFIED.**

The Department generally agrees with the recommendation, noting that some specific risks identified in the report appear less applicable to a state government agency and more suited for a private enterprise. The Department agrees with the intent and goal of this review and fully supports the approach to facilitate a collaborative exchange between CMS and the State Medicaid Agency.

The Department is committed to continuing its efforts in assessing and implementing strategies to enhance the operating efficiency and effectiveness of the Medicaid program. With the transition to Managed Care and subsequent program launches, the Department continues to take the opportunity to significantly enhance its governance practices and processes including those that identify project and operational risks and provide paths to mitigation. As supported by the noted operational credits in the report, the Department clearly recognizes that solely complying with Federal and State rules and regulations does not sufficiently reduce the possibility of patient harm nor sufficiently ensures available resources are best utilized to achieve program goals. As a next step in the continued maturation of our organizational oversight, an enterprise risk management program would ensure the development of adequate internal controls and regulatory compliance monitoring while also ensuring fiscal accountability is properly aligned with service delivery for better outcomes for all involved. To implement a successful enterprise risk management program will require investments in new staff roles, education and training

NC MEDICAID
NC DEPARTMENT OF HEALTH AND HUMAN SERVICES • DIVISION **OF HEALTH BENEFITS**

LOCATION: 1985 Umstead Drive, Kirby Building, Raleigh NC 27603
MAILING ADDRESS: 2501 Mail Service Center, Raleigh NC 27699-2501
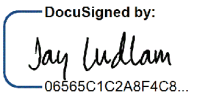www.ncdhhs.gov • TEL: 919-855-4100

AN EQUAL OPPORTUNITY / AFFIRMATIVE ACTION EMPLOYER

Risk Assessment of North Carolina's Medicaid Program (A-04-21-00127) 23

for the organization and its business partners, policy development/enhancement, and technology solutions for tracking and reporting. To achieve an assessment of *Low Risk* in a future review, the Department will work with the NC Legislature to secure the necessary resources needed to implement a formal enterprise risk management program to fully realize the mitigation efforts needed. We anticipate that while such an effort will be a multi-year project, the fiscal and operational rewards will far exceed the actual time and money spent to complete the effort.

We greatly appreciate the professionalism of your review staff and the opportunity to respond.

If you need additional information, please contact John Thompson at (919) 527-7701.

Sincerely,

DocuSigned by:

Jay Ludlam

06565C1C2A8F4C8...

Jay Ludlam
Deputy Secretary

cc: Melanie Bush, Deputy Medicaid Director
        Lotta Crabtree, Chief Legal Officer
        Sarah Gregosky, Chief Operating Officer
        Adam Levinson, Chief Financial Officer
        John E. Thompson, Chief Compliance Officer

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does it Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

📷 📘 ▶️ 𝕏 OIGatHHS

in HHS Office of Inspector General

[Subscribe To Our Newsletter](#)

[OIG.HHS.GOV](#)

Contact Us

For specific contact information, please [visit us online](#).

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov