Department: COMPLIANCE	Version #: 2
Title: Incident Reporting, Tracking and Resolution-Compliance, Fraud, Waste, Abuse, and HIPAA	
Process Owner: Chief Compliance Officer	Date Created: 2/26/2019 Last Reviewed Date: 7/23/2021
Document Type: Policy	Approver(s): Policy Review Committee
References: Chapter 21, Section 50.7 of the Medicare Managed Care Manual; 42 CFR. §§ 422.503(b) (4) (vi) (G); Chapter 9, Section 50.7 of the Prescription Drug Benefit Manual; 423.504(b) (4) (vi) (G); 45 CFR 164.	Date Approved: 8/2/2021

Printed copies are for reference only. Please refer to the S/Policies and Procedures for the most recent version.

Purpose: To ensure that ATRIO Health Plans (ATRIO) promptly responds to reports of, and detects, prevents, and corrects any noncompliance with any/all governing rules, regulations, contracts, or internal policies.

Summary: The Chief Compliance Officer, or designee, ensures an effective Compliance Program by tracking, reporting and monitoring ATRIO's compliance with the Centers for Medicare and Medicaid Services (CMS) contractual requirements, State Insurance regulation, the Health Insurance Portability and Accountability Act (HIPAA) and/or acts of potential or suspected fraud, waste and abuse (FWA).

Scope: This policy applies to all ATRIO Employees, vendors, Business Associates (BAs), and FDRs.

Definitions:

Business Associate: A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity (ATRIO).

Business Owner: The individual who oversees the specific operational area.

CMS: The Centers for Medicare & Medicaid Services. This is the agency within the Department of Health and Human Services (HHS) that is responsible for directing the national Medicare program.

ATRIO Employees: means any full-time employees, part-time employees, temporary employees, and volunteers employed by ATRIO or Atrio Holding Company, and Independent contractors.

FDR: First Tier, Downstream and Related Entities.

First Tier Entity: Any party that enters into a written arrangement, acceptable to CMS, with ATRIO to provide administrative services or health care services to an enrollee in ATRIO's Medicare Advantage or Dual Special Needs plan.

Downstream Entity: Any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the MA benefit or Part D benefit, below the level of the arrangement between ATRIO and a First Tier Entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services.

Related Entity: Any entity that is related to ATRIO by common ownership or control and: (a) performs some of ATRIO's management functions under contract or delegation; (b) furnishes services to Medicare enrollees under an oral or written agreement; or (c) leases real property or sells materials to ATRIO at a cost of more than $2,500 during a contract period.

FWA: Fraud, Waste and Abuse as defined in this section.

Fraud: Knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program; or to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program.

Waste: Overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare Program.

Abuse: Includes actions that may, directly or indirectly, result in unnecessary costs to the Medicare Program.

HIPAA: The Health Insurance Portability and Accountability Act that was passed by Congress in 1996. HIPAA mandates industry-wide standards for health care information on electronic billing and other processes and requires the protection and confidential handling of protected health information.

HIPAA Security: The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Non-compliance is failure to adhere to any laws, regulations, CMS requirements, contractual requirements, company policies and procedures, and/or ATRIO's Code of Conduct. Noncompliance also means actions that may result in adverse impact to ATRIO members. Non-compliance includes but is not limited to:

- Members receiving untimely services or inaccurate plan information
- Inappropriate denial of benefits, services, medications
- Members being inappropriately held responsible for cost-sharing
- Failure to provide members access to due process (appeal)
- Failure to adhere to regulatory timeframes

Generally, a CAP will be required when an issue of non-compliance results in one or more of the following:

- Regulatory or Contractual violations

- Measurable beneficiary/member harm (financial liability, inability to access drugs or benefits)
- Repetitive/systemic issues, rather than a one-time occurrence

Issues that fall outside of the above parameters should be documented and addressed by the applicable operational owner(s) in a Process Improvement Plan (PIP).

Security Incident: An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Policy:
Employees, BAs or FDRs are required to report (to Compliance) suspected, potential, or actual, fraud, waste and abuse (FWA) or noncompliance with any regulation or governing rules, including CMS and HIPAA.

ATRIO encourages members to report suspected, potential, or actual fraud, waste and abuse (FWA), noncompliance and HIPAA incidents by providing a variety of venues to do so. The venues include the compliance Hotline, calls to customer service, mailing complaints and online complaint form. All of these venues allow for anonymous submissions.

The Chief Compliance Officer may designate an individual to manage the incident reports. This includes, tracking and trending issues, gathering evidence if required, ensuring issues are addressed by Business Owners, escalating issues of ongoing noncompliance, and if appropriate, recommendations for a formal Corrective Action Plan and/or reporting to CMS Account Manager.

It is the Business Owners responsibility to maintain corrective action evidence and make it available to Compliance upon request.

All reported incidents are logged onto a Compliance Incident Tracking log, maintained by the Compliance Department. The Chief Compliance Officer or their designee logs and oversees the resolution of the incident.

Procedure:
Reporting: When an ATRIO Employee, BA, vendor, or FDR detects or suspects an issue of noncompliance, FWA, or HIPAA non-compliance, they are required to report the incident to Compliance. The incident may be reported by completing an Incident Report (IR) form or through any media and may be reported anonymously.

If known, the report should include:

- The date the issue occurred;
- How it was identified;
- The date it was identified;
- A root cause analysis;
- How many members are affected; and
- Corrective Actions

Compliance Review: The Chief Compliance Officer or their designee will review all reported incidents of actual or suspected noncompliance and FWA received via phone, mail, email or in person to determine the validity and severity of the issue.

- All reported incidents are logged onto a Compliance Incident Tracking log and tracked until the issue has been corrected.
- The investigation of the incident will be initiated as quickly as possible, but not later than 2 weeks after the date the potential noncompliance.
- FWA investigations that cannot be completed within 30 days of the date the potential FWA is identified, it should be forwarded to the I-MEDIC, regardless of whether or not the investigation is complete.

Review of each incident reported may include, but is not limited to, the following:

- Has this or similar issues been reported previously?
- Are the corrective actions appropriate to prevent future reoccurrences?
- Are the timelines for the corrective actions timely?
- Is there a member impact and if so, what type?
- Do we need a Beneficiary Impact Analysis?
- Does it require member notification?
- How was the issue identified and whether monitoring is in place?
- Is there additional monitoring that is needed?

The Chief Compliance Officer or their designee may seek assistance from internal and external subject matter experts such as physicians, pharmacists, business partners, coding experts, attorneys, law enforcement, and government integrity contractors.

At any point in the investigation, the Chief Compliance Officer or their designee may elect to suspend payments to a member or provider suspected of committing noncompliance or FWA. Payment for claims related to the incident under investigation may be held until the investigation is completed.

If a systemic deficiency, significant noncompliance with federal and state law or CMS guidance, actual or a high potential of member harm, or significant potential for regulatory fines or sanctions have been identified; Compliance may require a formal Corrective Action Plan (CAP).

- Reported to CMS Account Manager, if the issue is determined by the Chief Compliance Officer to be a significant issue of noncompliance;
- Referred to law enforcement and/or MEDIC(s), OIG, OCR, FCC, or a combination of these entities.

Resolution: The Chief Compliance Officer or the designee will track the actions identified and contact the Business Owner to ensure they have been completed. At times, the action dates may be changed, due to delays of completion. The designee will escalate the issue to the Chief Compliance Officer when there are concerns that the issue is not being addressed and noncompliance is continuing to occur.

If a Corrective Action Plan (CAP) is required, ATRIO staff will follow the process outlined in the CAP Work Instructions.

If a potential HIPAA breach has occurred, the issue should be reported to the Privacy Officer.

If overpayments or inappropriate payments are identified during the investigation Claims will be notified.

If there is reason to believe that a member or provider may have committed fraud or if serious quality of care are alleged, the Chief Compliance Officer or their designee may refer the case to regulatory agencies and/or law enforcement. Examples of agencies to which cases may be referred to include, but are not limited to:

- The Office of Inspector General (OIG)
- The Centers for Medicare & Medicaid Services (CMS)
- Medicare Drug Integrity Contractors (I-MEDIC)
- The Department of Labor
- Appropriate state agencies
- Local law enforcement
- Appropriate State Licensing Board
- Department Financial Regulation
- Office of Civil Rights

The Chief Compliance Officer or Compliance staff may recommend termination of a provider's contract.

If the incident of noncompliance or FWA involves an employee to the extent that corrective action is recommended, the Chief Compliance Officer or their designee will consult with Human Resources and will notify the department's management as appropriate.

- Any corrective actions taken will depend on the severity of the incident and will be in accordance with ATRIO Human Resources policies and procedures.

Record Retention:
The Compliance Department will maintain the documents related to an incident for a period of 10 years.

Related Policies & Procedures:
Code of Conduct
Record Retention Policy
WI_HIPAA Breach Notification for unsecured Protected Health Information
WI_CAP for Compliance and Business Owners