Department: COMPLIANCE	Version #: 5
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: 1/15/2024
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: 1/23/2024

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 potential or actual non-compliance with any/all governing rules, regulations, contracts, or internal policies.

Summary: The Chief Compliance Officer or designee, ensures an effective Compliance Program by tracking, monitoring, and reporting ATRIO's reports of potential or actual non-compliance with the Centers for Medicare and Medicaid Services (CMS) contractual requirements, State's 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 (including service-area-contractors).

Definitions:

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

Breach: Generally, impermissible use or disclosure under HIPAA that compromises the security or privacy of the protected health information (PHI). An impermissible use or disclosure of PHI is presumed to be a Breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment.

A "Breach" has not occurred if: (a) the unintentional acquisition, access, or use of PHI was made by a workforce member or person acting under the authority of ATRIO or its Business Associate, and if such acquisition, access, or use was made in good faith and within the scope of authority; (b) the inadvertent disclosure of protected health information was made by a person authorized to access protected health information at ATRIO or its Business Associate to another person authorized to access protected health information at ATRIO or its Business Associate, or organized health care arrangement in which ATRIO participates; or (c) ATRIO or its Business Associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

Business Associate (BA): 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). A Business Associate may be deemed an FDR; however, an FDR is always a Business Associate.

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

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

First Tier, Downstream and Related Entities (FDR):

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.

Fraud, Waste and Abuse (FWA) 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.

The Health Insurance Portability and Accountability Act (HIPAA. 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.

I-MEDIC through HPMS: The Investigations Medicare Integrity Contractor performs Medicare Parts C & D investigations on prescribers, pharmacies, and beneficiaries. Its primary focus is on complaint intake and response, assessing leads, data analysis and investigative and administrative actions.

Non-compliance: Failure to adhere to any laws, regulations, CMS requirements, contractual requirements, company policies and procedures, and/or ATRIO's Code of Conduct. Non-compliance 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.

Potential Non-compliance: When a situation or issue has been identified, but the research has not been completed to determine if actual Non-compliance, as defined above, has occurred.

Protected Health Information (PHI): Individually identifiable health information that is: (1) transmitted by electronic media; (2) maintained in electronic media; or (3) transmitted or maintained in any other form or medium. PHI excludes Individually Identifiable Health Information regarding a person who has been deceased for more than 50 years.

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, and FDRs are required to report suspected, potential, or actual FWA or Non-compliance with any regulation or governing rules, including CMS and HIPAA.

ATRIO expects employees, FDRs, and plan members to report suspected, potential, or actual FWA, Non-compliance and HIPAA incidents. There are a variety of ways to report, which include calling the Compliance Line (877)-309-9952, Customer Service (877)-672 8620, mailing a letter, and/or completing an online complaint form (see below).

ATRIO employees or FDR staff may use any of the above to report. However, the preferred method for Employees and FDRs to report is the Incident Report form, which provides all the necessary information. All these reporting paths allow for anonymous submissions.

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

The initial incident report should be completed within as soon as possible (preferably within 72) hours after discovery or notification of the following.

- When Non-compliance is identified by the business owner or staff
- Non-compliance identified through the CMS/HPMS Complaint Tracking Model
- For any system issues potentially affecting members
- For any Notice of Non-Compliance resulting from external audit
- For any internal audit “finding” CAR or ICAR.

When a Corrective Action Plan is implemented for any of the above, an incident report is not required.

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 Compliance Officer or their designee logs and oversees the resolution of the incident.

Procedure:

Reporting to Compliance: When an ATRIO Employee, BA, vendor, FDR, or any individual detects or suspects an issue of Non-compliance, FWA, or HIPAA non-compliance, the issue should be reported to Compliance.

Regarding HIPAA breaches specifically:
When any employee or FDR employee becomes aware of a HIPAA Breach or suspected Breach of PHI, he/she must notify the Compliance Department immediately or as soon as reasonably possible. Members are encouraged to report issues to ATRIO to investigate. This includes suspicious or suspected scam calls and receiving someone else's information in the mail.

When a BA becomes aware of a Breach of PHI, the BA is required to notify ATRIO without unreasonable delay after the discovery of the Breach. The BA is required to cooperate fully with the Compliance Department in the risk assessment and corrective actions.

All incidents Potential or Actual Non-compliance, FWA or HIPAA Breach may be reported to compliance through the various methods, which include:

- Complete and send to Compliance an Incident Report (IR) form.
- Send an e-mail or instance message to the Compliance staff.
- Call Compliance staff
- Schedule a face-to-face meeting with Compliance staff
- Call ATRIO's Compliance Line
- Mail a letter.
- Complete an online form at atriohp.com.

All incidents may be reported anonymously. Anonymous reports may be made by:
- Call ATRIO Compliance Line at **1-877-309-9952**
- Mail: ATRIO Health Plans, PO Box 12645, Salem, OR 97309
- ATRIO's Website, Online Incident Reporting Form: http://www.atriohp.com
- Omit the reporter's name from the Incident Reporting form.

If known, the report should include:
- The date the issue occurred.
- How it was identified.
- The date it was identified.
- The contract number(s) impacted.
- A root cause analysis.
- How many members and claims are affected; and
- Corrective actions

All the information that is required is included in the Incident Reporting form.

Compliance Review:

The Compliance Officer or their designee will review all reported incidents of actual or suspected Non-compliance 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 Non-compliance.

- FWA investigations wherein either the time or the resources to investigate the potential fraud or abuse in a timely manner are unavailable, the matter should be referred to the I-MEDIC within 30 days of the date of the identification of the FWA so that the potential FWA activity does not continue.

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 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 Compliance Officer or their designee may elect to suspend payments to a member or provider suspected of committing Non-compliance or FWA. Payment for claims related to the incident under investigation may be held until the investigation is completed.

If a systemic deficiency, significant Non-compliance 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).
- Report the issue to the CMS Account Manager if the issue is determined by the Compliance Officer to be a significant issue of Non-compliance.
    - When it is determined that we will report (self-disclose) to the CMS Account Manager the business owner is required to complete the Beneficiary Impact Analysis form-which contains additional details needed to report.
- Refer the case to regulatory agencies and/or law enforcement.

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

- Office of Inspector General (OIG)
- Centers for Medicare & Medicaid Services (CMS)
- Medicare Drug Integrity Contractors (I-MEDIC)
- Department of Labor
- Federal Communications Commission (FCC)
- Office for Civil Rights (OCR)
- Appropriate state agencies, such as Department of Financial Regulation (DFR)
- Local law enforcement
- Appropriate State Licensing Board

Dashboard and reporting out:

When an incident is identified as high risk and potential member impact, the Compliance Officer or their designee may escalate the issue to the executive staff.

Internal Reporting:
Monthly the dashboard is updated to include the number of incidents reported by source.

Quarterly, the dashboard is presented to the Internal Compliance Committee. In January 2024, the dashboard report will include how many of the incidents resulted in non-compliance and the number of beneficiaries impacted. Not all reported incidents will result in Non-compliance or member Impact. This information is included in the slide deck presented to the Board of Directors quarterly.

External Reporting to CMS Account Manager.
The number of incidents Compliance received and the source of the incidents **charts in the dashboard are replaced with** total number of incidents self-disclosed to CMS and the number of complaints received and resolved monthly through the HPMS Complaint Tracking Module platform.

Resolution:
The 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 in completion.

The designee will escalate the issue to the Compliance Officer when there are concerns that the issue is not being addressed and Non-compliance is continuing to occur.

If a CAP is required, ATRIO staff will follow the process outlined in the CAP Work Instructions.
Claims will be notified if overpayments or inappropriate payments are identified during the investigation.
The Compliance Officer or Compliance staff may recommend termination of a provider's contract.

If the incident of Non-compliance, HIPAA Breach or FWA involves an Employee, to the extent that disciplinary action is recommended, the Compliance Officer or their designee will consult with Human Resources and will notify the department's management as appropriate.

- Any corrective and/or disciplinary 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:
Incident Reporting form
Beneficiary Impact Analysis form
Code of Conduct
Record Retention Policy
Compliance Program Disciplinary Standards Policy
WI_Corrective Action Plans
WI_Managing Reported Non-Compliance, FWA & HIPAA Incidents
Employee Handbook.