2026 Compliance and Risk Management Plan & Code of Conduct

Trillium Health, Inc.
259 Monroe Avenue
Rochester, New York 14607
585.545.7200 | trilliumhealth.org

Table of Contents

I. Executive Summary

Why Have a Compliance Program?

Trillium's Compliance Program is necessary because it:

- Stops fraud
- Protects patient privacy
- Nurtures an ethical culture
- Prevents conflicts of interest
- Ensures proper credentialing
- Identifies and prevents waste
- Furthers accurate billing and coding
- Assists in obeying state and federal laws
- Maintains and promotes high quality care
- Strives to promote the use of best practices in management and board governance.

Trillium's Code of Conduct requires you to:

- Act fairly
- Act ethically
- Act honestly
- Act as a team
- Report a conflict of interest that you may have
- Treat patients and one another with respect at all times
- Identify ways to do things better in your department and take action
- Report problems immediately to your supervisor, directly to the Compliance Director or the Chief Compliance and Risk Officer, or take advantage of our anonymous compliance hotline options.

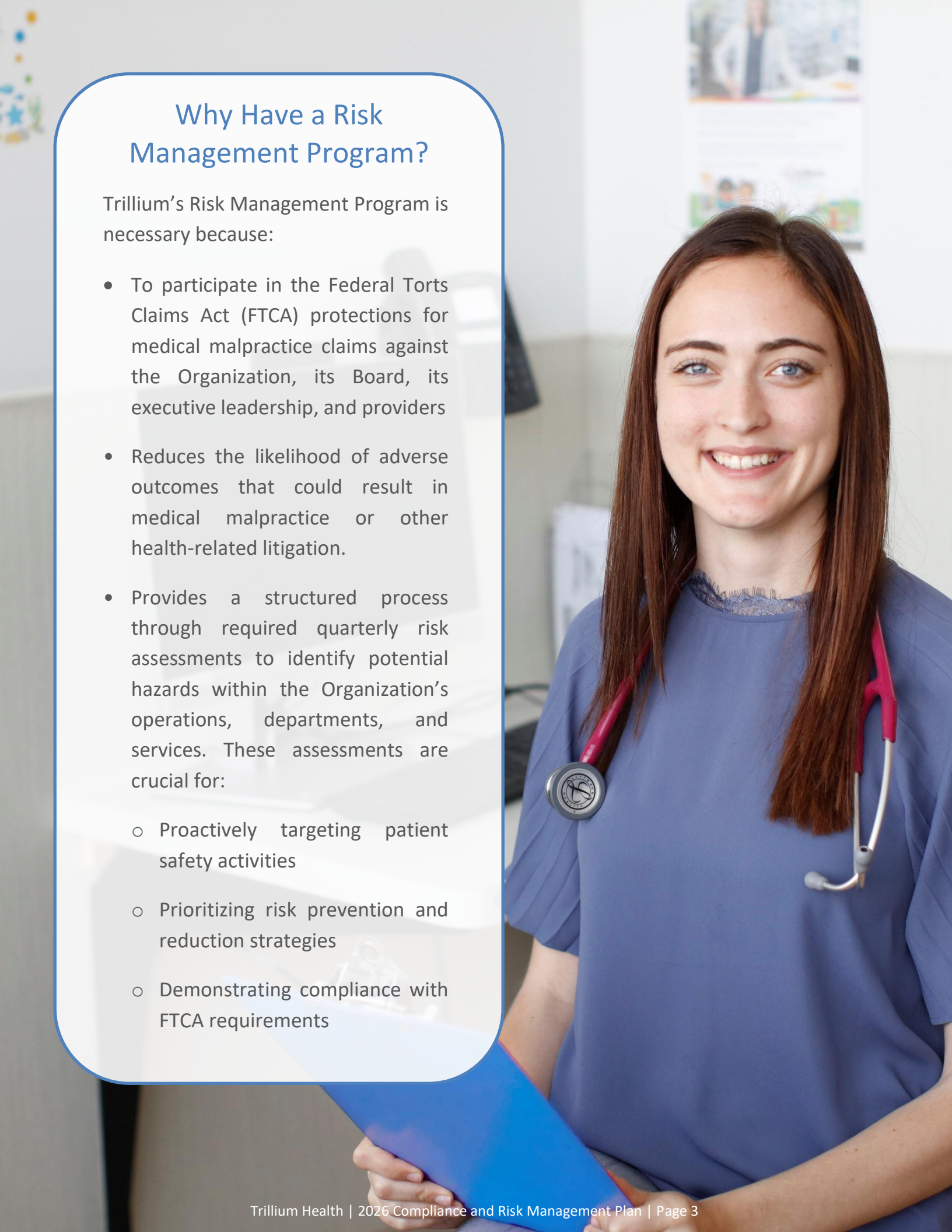
Trillium Health's Compliance Program applies to:

- Vendors
- Contractors
- Consultants
- All staff no matter the title or position
- Board of Directors

Why Have a Risk Management Program?

Trillium's Risk Management Program is necessary because:

- To participate in the Federal Torts Claims Act (FTCA) protections for medical malpractice claims against the Organization, its Board, its executive leadership, and providers
- Reduces the likelihood of adverse outcomes that could result in medical malpractice or other health-related litigation.
- Provides a structured process through required quarterly risk assessments to identify potential hazards within the Organization's operations, departments, and services. These assessments are crucial for:
    - Proactively targeting patient safety activities
    - Prioritizing risk prevention and reduction strategies
    - Demonstrating compliance with FTCA requirements



II. Introduction

Trillium Health, Inc. ("the Organization") is a federally qualified health center ("FQHC") with a mission to promote health equity by providing affordable and extraordinary primary and specialty care, including LGBTQ health care. We are strongly committed to and have a longstanding reputation for lawful and ethical conduct. We take pride in earning the trust of those we serve, government regulators and one another.

The Affordable Care Act requires organizations that participate in federal health programs to have a formal compliance program. New York's Office of the Medicaid Inspector General ("OMIG") requires Medicaid providers to have a compliance program as well as a code of conduct. Additionally, in response to the many laws, rules, and regulations governing healthcare, the Organization has established a comprehensive compliance program to help us live up to our commitment to adhere to the highest ethical standards of conduct in all business practices.

This compliance and risk management plan is modeled after the seven elements identified by OMIG for an effective compliance and risk management program. It also addresses concerns as outlined in the Deficit Reduction Act ("DRA"), which requires the Organization to establish written policies and procedures to inform employees and others about certain federal and state false claims and whistleblower laws.

The goal of the Organization's compliance program is to prevent fraud, waste, and abuse while at the same time advancing the mission of providing affordable and extraordinary primary and specialty care. Our compliance efforts are aimed at prevention, detection, and resolution of variances.

Lastly, as an FQHC, Trillium is eligible to receive Federal Tort Claims Act protection, which requires Trillium to establish and maintain a Risk Management Program to reduce the likelihood of adverse outcomes that could result in medical malpractice or other health-related litigation. Specifically, the Plan requires Trillium to develop, review, and revise the organization's practices and protocols in light of identified risks and chosen loss prevention and reduction strategies.

The Seven Elements of the Organization's Compliance Plan are:

1. Written policies and procedures
2. Designation of a Compliance Officer/Committee
3. Training and education programs
4. Open lines of communication to the Responsible Compliance Position
5. Disciplinary policies to encourage good faith participation
6. A system for routine identification of compliance risk areas
7. A system for responding to compliance issues

The Key Elements of the Organization's Risk Management Program are:

1. Ongoing Risk Management Program, which includes:
    a. Quality Improvement/Quality Assurance
    b. Credentialing and Privelaging
    c. Claims Management
2. Ongoing Risk Management Procedures
3. Annual Healthcare Risk Management Training Plan
4. Quarterly Risk Assessments
5. Annual Report to the Board
6. Risk Manager Position Description
7. Risk Training for the Risk Manager

The Compliance Plan applies to the following areas:

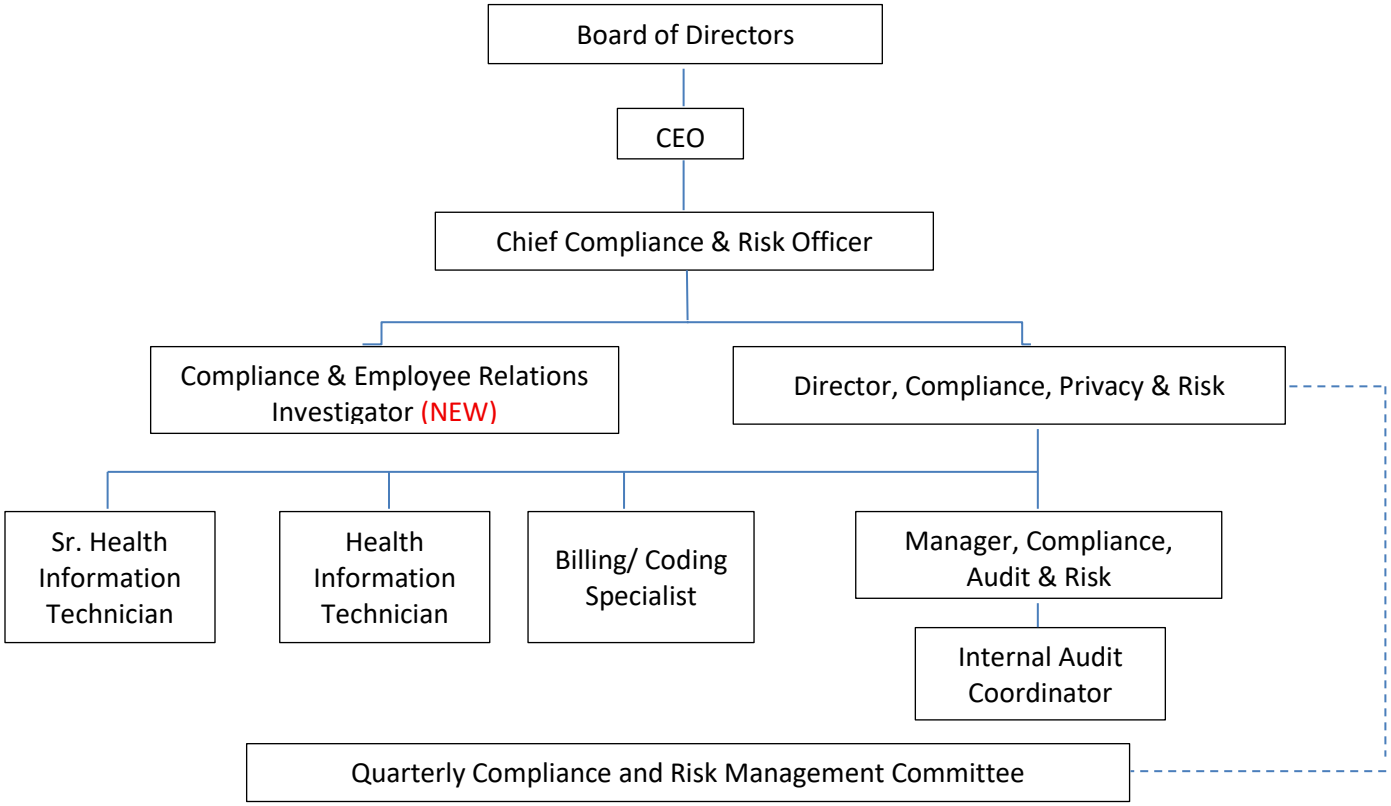
1. Billings
2. Payments
3. Ordered Services
4. Medical necessity
5. Quality of care
6. Governance
7. Mandatory reporting
8. Credentialing
9. Contractor, subcontractor, agent, or independent contract oversight
10. Other risk areas that are or should reasonably be identified by the provider through “organizational experience.”

III. Compliance and Risk Management Structure

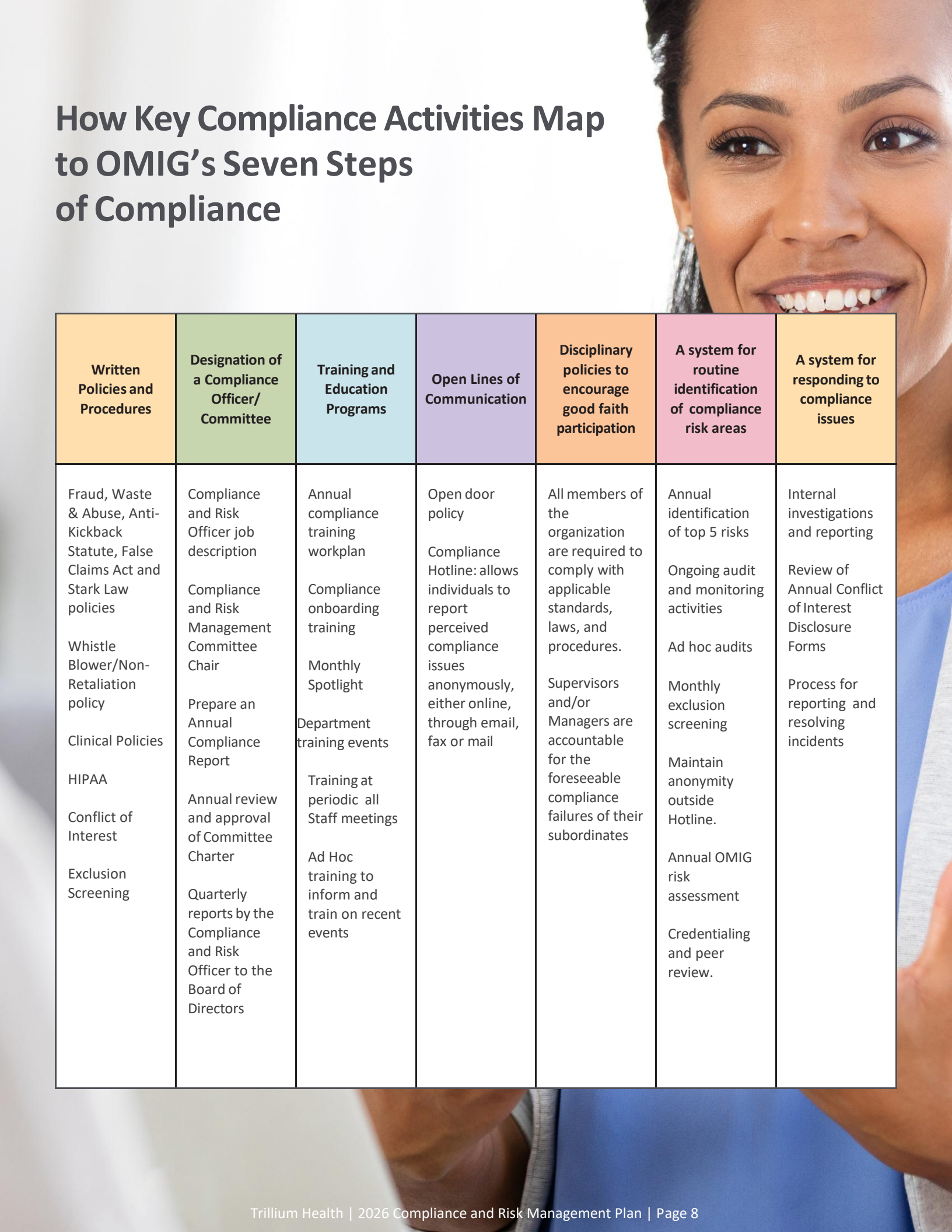
The Organization is required to have an effective compliance and risk management program as a condition of receiving payments from the Medicaid program. The Organization's compliance and risk management program imposes compliance requirements for contractors, agents, subcontractors, and independent contractors (Contractors) within the scope of the contracted authority and affected risk areas.

The compliance and risk management program starts with its board of directors, who must ensure the Organization operates in compliance with applicable Federal, state, and local laws and regulations. The board of directors provides direction to our CEO, who sets the tone for the Organization's compliance and risk management activities.

The Chief Compliance and Risk Officer works to ensure the Organization has the appropriate policies, procedures and processes in place to minimize its risk and further the Organization's mission to provide primary care services regardless of a person's ability to pay. In addition to the Chief Compliance and Risk Officer, the Compliance and Risk Management Team consists of the Director of Compliance, Privacy & Risk, a Compliance Audit & Risk Manager, an Internal Audit Coordinator, and three Health Information Technicians with one having a Medical Coding/Billing specialty. In 2026, the Organization will add a Compliance & Employee Relations Investigator resource, who will report directly to the Chief Compliance and Risk Officer. On a quarterly basis, the Chief Compliance and Risk Officer and the Director of Compliance meet with the Compliance and Risk Management Committee and provide updates on the department's activities and future plans, as well as review any new compliance concerns.



How Key Compliance Activities Map to OMIG's Seven Steps of Compliance



Written Policies and Procedures	Designation of a Compliance Officer/ Committee	Training and Education Programs	Open Lines of Communication	Disciplinary policies to encourage good faith participation	A system for routine identification of compliance risk areas	A system for responding to compliance issues
Fraud, Waste & Abuse, Anti-Kickback Statute, False Claims Act and Stark Law policies Whistle Blower/Non-Retaliation policy Clinical Policies HIPAA Conflict of Interest Exclusion Screening	Compliance and Risk Officer job description Compliance and Risk Management Committee Chair Prepare an Annual Compliance Report Annual review and approval of Committee Charter Quarterly reports by the Compliance and Risk Officer to the Board of Directors	Annual compliance training workplan Compliance onboarding training Monthly Spotlight Department training events Training at periodic all Staff meetings Ad Hoc training to inform and train on recent events	Open door policy Compliance Hotline: allows individuals to report perceived compliance issues anonymously, either online, through email, fax or mail	All members of the organization are required to comply with applicable standards, laws, and procedures. Supervisors and/or Managers are accountable for the foreseeable compliance failures of their subordinates	Annual identification of top 5 risks Ongoing audit and monitoring activities Ad hoc audits Monthly exclusion screening Maintain anonymity outside Hotline. Annual OMIG risk assessment Credentialing and peer review.	Internal investigations and reporting Review of Annual Conflict of Interest Disclosure Forms Process for reporting and resolving incidents

IV. Written Policies & Procedures

A. OVERVIEW

The Organization has a process for drafting, revising, and approving written policies. These policies must be accessible and applicable to all Affected Individuals. Affected Individuals means all persons who are affected by the organization's risk areas, including employees, the chief executive and other senior administrators, managers, contractors, agents, subcontractors, governing body, and corporate officers.

The written compliance policies and procedures provide a clear explanation of the Organization's compliance and quality goals and provide clear and understandable mechanisms and procedures designed to achieve those goals in compliance with Federal, State, and other program requirements and standards.

The Organization has specific, individual policies for an array of matters, ranging from proper documentation of services to whistleblower protections. These policies and procedures are available online at the Organization's Policy Tech site. In addition to compliance expectations, the Organization's policies also describe our fundamental principles and values, and commitment to conduct its business in an ethical manner. Also, the Organization's policies describe the structure of the compliance program, including the responsibilities of all Affected Individuals in carrying out the functions of the compliance program. Our written policies include specific guidance on dealing with potential compliance issues and communicating compliance issues to the appropriate compliance personnel. Lastly, the Organization's Investigation policy includes:

- a description of the procedures for documenting the investigation and the resolution or outcome; and
- the potential consequences to Affected Individuals who fail to comply with the Organization's written policies, or state and federal laws, rules, and regulations.

The Organization's Fraud, Waste and Abuse policy addresses compliance with all applicable Federal and State laws pertaining to fraud, waste, and abuse in Federal health care programs. These policies include Section 6032 of the Deficit Reduction Act of 2005, which requires the Organization to establish written policies that provide detailed information about fraud, waste, and abuse in Federal health care programs. These policies must be disseminated to employees, agents, and contractors. Additionally, the Organization's agents and contractors must adopt and abide by the policies.

The Organization reviews its policies on an annual basis.

B. CONFLICT OF INTEREST POLICY AND DISCLOSURE STATEMENT

The Organization is required to ensure that it adheres to the highest standards of ethical conduct by identifying instances in which an independent observer might reasonably conclude that the potential for individual or institutional conflict could influence decision-making or carrying out responsibilities. The Organization has a Conflict of Interest Policy that is based upon full disclosure and appropriate management of any possible conflict of interest. The policy requires staff members, including full-time, part-time, contract, consultants, and those who provide goods and services to the health center, volunteers, Board of Directors, and volunteers of a Board Committee, to conduct their business according to the highest ethical standards of conduct and to comply with all applicable laws.

The Organization requires individuals to complete the Annual Conflict of Interest Disclosure Form to assist in identifying and evaluating potential conflicts of interest. Also, individuals are required to disclose any actual, potential, or perceived conflicts as they arise during their affiliation or employment with the Organization. The forms are reviewed on an annual basis or when the need to complete the statement arises (new hires or changed circumstances). It is the responsibility of everyone to have a working knowledge of these policies and procedures and refer to them. Also, the Organization has a written process for addressing related-party transactions as part of its Conflict of Interest policy.

C. RELATED PARTY TRANSACTIONS

The Organization requires people to disclose related party transactions, which are business or financial transactions between the Organization and an entity or individual that has a close relationship with the Organization. The organization's board must approve the transaction to ensure it is conducted in a fair and transparent manner and in the Organization's best interests. In some instances, the board may impose conditions in connection with the related party transaction. All related parties must abstain from all discussion, deliberations, voting related to the engagement, and all ongoing oversight responsibilities once the agreement has been formalized.

V. Governance

OTHER WRITTEN POLICIES AND PROCEDURES

A. ANNUAL WORK PLAN

Every year, the Chief Compliance and Risk Officer will prepare an Annual Compliance and Risk Management Work Plan ("Work Plan") after reviewing the latest New York State Office of the Medicaid Inspector General and the United States Office of Inspector General priorities, recent enforcement activities, recent internal and external audit findings, and hot topics that generate additional scrutiny. Additionally, the Chief Compliance and Risk Officer will obtain input from the Chief Executive Officer, the Director of Compliance, Risk, and Privacy, the staff Compliance and Risk Management Committee, and various departments through interviews and a durable process for weighing the likelihood and impact of potential compliance issues. The Work Plan will include the top five risk areas of concern.

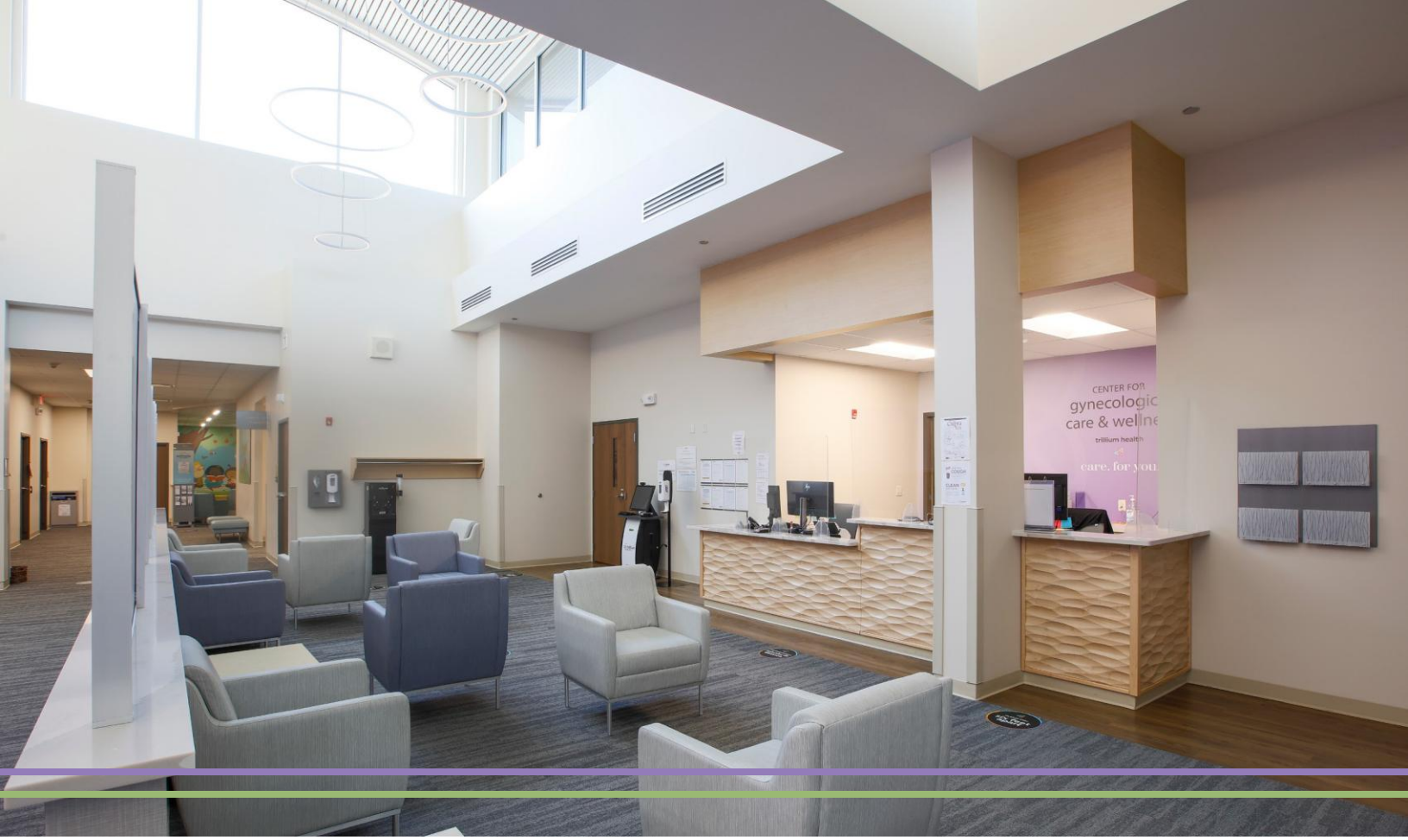
FOR 2026, THE TOP FIVE RISK AREAS ARE:

- IT Security
- Information Privacy
- Billing
- Grant Management
- Vendor Management

Additionally, the Work Plan includes a list of areas that the Compliance and Risk Management Department will audit and monitor. The Compliance and Risk Management Department may add additional monitoring audits to its duties in response to new and emerging risks. The Compliance and Risk Management Department and audited departments will review the audit findings and develop audit responses to address findings. The parties will develop remediation plans and associated timelines. The Compliance and Risk Management Department will conduct follow-up on remediation activities and report progress to the Chief Executive Officer and the Chief Compliance and Risk Officer. Additionally, the Compliance and Risk Management Department will provide assistance with external audits from federal, state, and other oversight organizations.

B. AD HOC POLICY, PROCEDURE, AND TRAINING DEVELOPMENT

From time to time, the Compliance and Risk Management Department will work with other departments to develop and revise policies, procedures, and training to reflect new legal requirements and new concerns that may arise.



C. NON-INTIMIDATION AND NON-RETALIATION POLICIES

The Organization will protect whistle-blowers from retaliation. The Organization will not retaliate against employees who, in good faith, have raised a complaint against some practice of the Organization, or of another individual or entity with whom the Organization has a business relationship, on the basis of a reasonable belief that the practice is in violation of law, or a clear mandate of public policy.

Staff, vendors, interns, contractors, and Board Members are obligated to report to the Chief Compliance and Risk Officer any activity he, she, or they believe to be inconsistent with the Organization's policies or state and federal law. The Organization has a Whistleblower policy which is intended to encourage and enable employees and others to raise serious concerns within the Organization, prior to seeking resolution outside of the Organization. The policy protects employees who, in good faith, report an ethics violation from harassment, retaliation, or adverse employment consequence. Any employee who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment.

Reports of violations or suspected violations will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation. The Chief Compliance and Risk Officer will notify the sender and acknowledge receipt of the reported violation or suspected violation within five business days. All reports will be promptly investigated, and appropriate corrective action will be taken if warranted by the investigation. Additionally, the Organization has a process for the anonymous submission of perceived violations.

VI. Designation of a Compliance and Risk Officer and Compliance and Risk Management Committee

The OMIG requires the organization to designate a compliance officer to carry out and enforce compliance activities. Trillium's risk management program requires Trillium to designate a risk manager. The Compliance and Risk Officer is the focal point for the organization's compliance and risk management program and is responsible for the day-to-day operation of the compliance and risk management program. The compliance and risk officer functions as an independent and objective person that reviews and evaluates organizational compliance, risk, and privacy/confidentiality issues and concerns. The compliance and risk officer's main duties include coordination and communication of the compliance and risk management plan; this involves planning, implementing, and monitoring the program.

The compliance and risk officer reports directly to and is accountable to the chief executive officer. However, such designation does not hinder the compliance and risk officer in carrying out their duties and having access to the chief executive and governing body.

The Organization designates the Senior Vice President, Compliance, Technology, Privacy and Regulatory Affairs to serve as the Chief Compliance and Risk Officer and coordinator of all compliance and risk management activities.

A. RESPONSIBILITIES OF THE CHIEF COMPLIANCE AND RISK OFFICER

- Handle inquiries by employees, volunteers, affiliates, consumers, and family members regarding compliance and risk management issues
- Chairing the Compliance and Risk Management Committee and serving as a spokesperson for the Committee.
- Overseeing and monitoring the adoption, implementation, and maintenance of the compliance and risk management program and evaluating its effectiveness.
- Drafting, implementing, and updating no less frequently than annually or, as otherwise necessary, to conform to changes to Federal and State laws, rules, regulations, policies, and standards, a compliance and risk management workplan which outlines the organization's strategy for meeting requirements in the coming year.
- Reporting directly, on a regular basis, but no less frequently than quarterly, to the Compliance and Risk Management Committee, the Chief Executive Officer, and the Board of Directors on the progress of implementation and maintenance of compliance and risk management initiatives, corrective actions, and recommendations to reduce the vulnerability to allegations of fraud, waste, and abuse.
- Developing, coordinating, and participating in a multifaceted educational and training workplan that focuses on the elements of the compliance and risk management program and seeks to ensure that all employees are knowledgeable of, and comply with, pertinent federal, state, and private payer standards
- Ensuring that employees, vendors, and the Board of Directors do not appear on any of the Federal or State "excluded, debarred or suspended" listings published by Medicare and Medicaid.

- Ensuring that all Providers/Care Management Staff are informed of compliance and risk management program standards with respect to coding, billing, documentation, etc.
- Investigating and independently acting on matters related to the compliance and risk management program, including designing and coordinating internal investigations and documenting, reporting, coordinating, and pursuing any resulting corrective action with all internal departments, contractors, and the State.
- Reviewing the results of compliance and risk management audits, including internal reviews of compliance, risk management, independent reviews, and external compliance audits.
- Develop policies and programs that encourage managers and employees to report suspected fraud and other improprieties without fear of retaliation. (See Whistleblower Policy)
- Interact with external legal counsel to discuss the Organization's initiatives on regulatory compliance and risk management as necessary.
- Reviewing and revising the compliance and risk management program, the associated written policies and procedures, and Code of Conduct, to incorporate changes based on the organization's experience and promptly incorporate changes to Federal and State laws, HRSA, FTCA, rules, regulations, policies, and standards
- Developing and distributing all written compliance and risk management policies and procedures to all affected employees.

B. COMPLIANCE AND RISK MANAGEMENT COMMITTEE

The Organization will designate a Compliance and Risk Management Committee to coordinate with and advise the Chief Compliance and Risk Officer to ensure that the organization is conducting its business in an ethical and responsible manner consistent with its compliance and risk management program. The Organization outlines the duties, responsibilities, membership, designation of a chair, and frequency of meetings in a compliance and risk management committee charter.

The Compliance and Risk Management Committee membership at a minimum consists of senior managers and meets no less frequently than quarterly and shall no less frequently than annually review and update the Compliance and Risk Management Committee charter.

The Compliance and Risk Management Committee reports directly to and is accountable to the Chief Executive Officer and Board of Directors.

The Functions of the Compliance and Risk Management Committee

- Analyze the Organization's regulatory environment, the legal requirements with which it must comply, and specific risk areas.
- Coordinate with the compliance and risk officer to ensure that the written policies and procedures, and standards of conduct are current, accurate, and complete, and that the training topics are timely reviewed, updated as necessary, and completed.
- Coordinate with the Compliance and Risk Officer to ensure communication and cooperation by Affected Individuals on compliance-related issues, internal or external audits, or any other compliance and risk management function or activity.
- Advocate for the allocation of sufficient funding, resources, and staff for the Compliance and Risk Officer to fully perform their responsibilities.
- Recommend and monitor the development of internal systems and controls to implement standards, policies, and procedures as part of the daily operations.
- Determine the appropriate strategy/approach to promote compliance and risk management with the program and detection of any potential problems, violations, risks, or opportunities for improvement.
- Develop a system to solicit, evaluate, and respond to complaints and problems.

VII. Conducting Effective Training and Education

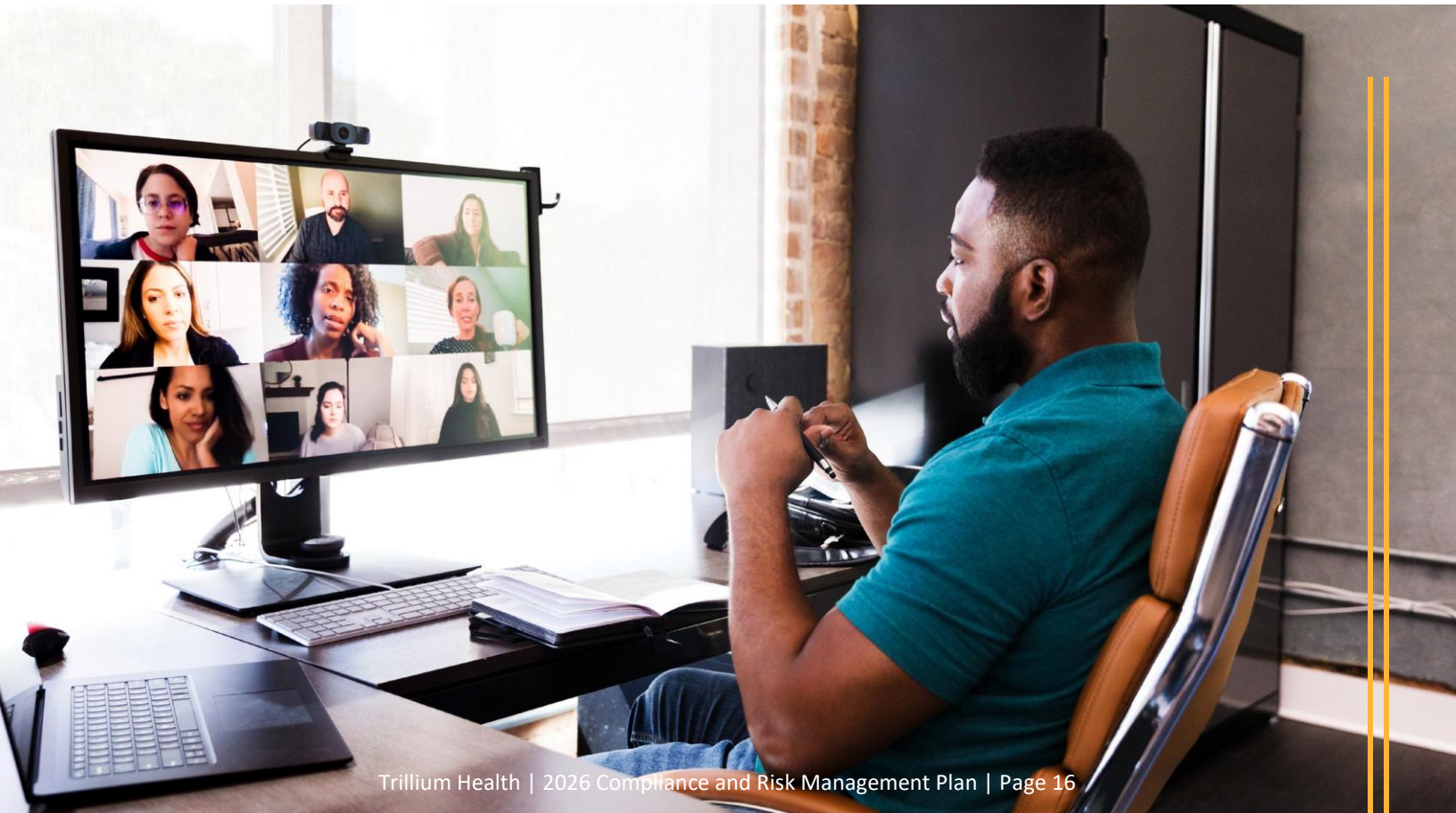
An effective Compliance and Risk Management Program is rooted in an active and adaptive education and training program. Active education and training are designed to teach each person how to carry out their responsibilities effectively, efficiently, and in compliance with statutory and regulatory compliance and risk management requirements. Adaptive education and training are designed to be responsive to the educational needs of the Organization's workforce identified through internal and/or external reviews, audits, or compliance and risk management assessments or by government notices, alerts, and/or other advisory statements.

The Organization maintains a training workplan that outlines the topics, timing, and frequency, how it is tracked, and how the effectiveness of the training is periodically evaluated. The organization requires all Affected Individuals to attend specific training as part of their orientation and no less frequently than on an annual and as needed basis thereafter.

Training includes training in federal and state statutes, regulations, program and risk management requirements, and corporate ethics. The training emphasizes the Organization's commitment to compliance and risk management with these legal and risk management requirements and policies.

The training programs will include sessions highlighting the Organization's Compliance and Risk Management Program, summaries of fraud and abuse laws, discussions of coding requirements, claim development, and claim submission processes that reflect current legal and program standards.

The Chief Compliance and Risk Officer or other designated staff member will document the attendees, the subjects covered, and any materials distributed at the training sessions.



BASIC TRAINING AT MINIMUM WILL INCLUDE:

- The organization's risk areas and organizational experience,
- The role of the compliance and risk management officer and the compliance and risk management committee,
- Overview of the Organization's regulatory environment;
- Fraud, waste, and abuse;
- The Organization's compliance and risk management structure;
- Coding and billing requirements, where applicable
- Claim development and the submission process, where applicable
- The seven elements of compliance;
- Where to find the compliance and risk management plan and policies and procedures on the Organization's SharePoint site;
- Key laws and regulations to be aware of;
- The Organization's commitment to non-retaliation;
- Compliance hotline information for making anonymous complaints; and
- How Affected Individuals can ask questions and their duty to report suspected or actual misconduct and compliance-related issues, to the Compliance and Risk Officer and senior management.

VIII. Developing Effective and Open Lines of Communication

A. OPEN LINES OF COMMUNICATION

Open lines of communication encourage everyone to express their compliance, quality, and other concerns and/or suggestions for improvement without fear of retaliation. Open communication is essential to maintaining an effective Compliance and Risk Management Program and enables the Organization to learn about issues that may arise, generating faster responses and quicker fixes. Additionally, open communications allow the Organization to address small problems before they become big ones.

Any potential problem or questionable practice which is, or is reasonably likely to be, in violation of, or inconsistent with, federal or state laws, rules, regulations, or directives or the Organization rules or policies relative to the delivery of healthcare services, or the billing and collection of revenue derived from such services, and any associated requirements regarding documentation, coding, supervision, and other professional or business practices must be reported to the Chief Compliance and Risk Officer.

Confidential lines of communication are accessible to all affected individuals and allow for questions to be asked and for compliance and risk management issues to be reported. The method of reporting allows for anonymous reporting of potential fraud, waste, and abuse as well as allows for reporting issues directly to the Compliance and Risk Management Officer.

Confidentiality of persons reporting issues shall be maintained unless the matter is subject to a disciplinary proceeding, referred to, or under investigation by MFCU, OMIG or law enforcement, or disclosure is required during a legal proceeding, and such persons shall be protected under the organization's policy for non-intimidation and non-retaliation.

The Compliance Hotline

Any person who has reason to believe that a potential problem or questionable practice is in existence should report the circumstance to the Chief Compliance and Risk Officer. Such reports may be made verbally or in writing and may be made on an anonymous basis. The Organization utilizes an external vendor, The Compliance Hotline, so that employees may anonymously consult with the Chief Compliance and Risk Officer with questions or report violations though the following mediums

ONLINE: _____ my.compliancehotline.com/report/trilliumhealth
EMAIL: _____ reports@compliancehotline.com
PHONE: _____ 1 (800) 561-0798
FAX: _____ 1 (800) 519-6369
MAIL: __ Trillium Health c/o Exclusion Screening 2121 e NW #C2E Washington, DC 20007

B. HHS-OIG FRAUD HOTLINE

Fraud or Abuse in connection with Federal health care programs may be confidentially reported to HHS-OIG Fraud Hotline: 1 (800) HHS-TIPS.

The Chief Compliance and Risk Officer will promptly document and investigate reported matters that suggest substantial violations of policies, regulations, statutes, or program requirements to determine their veracity.

The Chief Compliance and Risk Officer will work closely with legal counsel who can provide guidance regarding complex legal and management issues.

C. EXIT INTERVIEWS

As a further reflection of the organization's efforts to nurture an ethical culture, exit interviews with the Director, Compliance, Privacy & Risk are available to any employee or Board member leaving the Organization. Coding, supervision, and other professional or business practices must be reported to the Chief Compliance and Risk Officer.

IX. Disciplinary Standards

All Affected Individuals of the Organization will be held accountable for failing to comply with applicable standards, laws, and procedures. Supervisors and/or Managers will be held accountable for the foreseeable compliance failures of their subordinates.

The Supervisor or Manager will be responsible for taking appropriate disciplinary actions in the event an employee fails to comply with applicable regulations or policies. The disciplinary process for violations of compliance programs will be administered according to Organization protocols (generally verbal warning, written warning, suspension without pay, and may lead to termination) depending upon the seriousness of the violation. The Chief Compliance and Risk Officer is to be consulted and may consult legal counsel in determining the seriousness of the violation. However, the Chief Compliance and Risk Officer should never be involved in imposing discipline.

If the deviation occurred due to legitimate, explainable reasons, the Chief Compliance and Risk Officer and supervisor/manager may want to limit disciplinary action or take no action. If the deviation occurred because of improper procedures, misunderstanding of rules, including systemic problems, the Organization should take immediate action to correct the problem.

When disciplinary action is warranted, it should be prompt, fairly, and consistently applied to all levels of personnel according to written standards of disciplinary action.

Within 30 working days after receipt of an investigative report, the supervisor and/or V.P. of Human Resources or their designee shall determine the action to be taken upon the matter. The action may include, without limitation, one or more of the following:

1. Dismissal of the matter.
2. Verbal counseling.
3. Issuing a warning, a letter of admonition, or a letter of reprimand.
4. Entering into and monitoring a corrective action plan. The corrective action plan may include requirements for individual or group remedial education and training, consultation, proctoring, and/or concurrent review.
5. Reduction, suspension, or revocation of clinical privileges.
6. Suspension or termination of employment.
7. Modification of assigned duties.
8. Reduction in the amount of salary compensation.

The President/CEO or V.P., Chief Medical Officer shall have the authority to, at any time, suspend summarily the involved employee or contractor's privileges or to summarily impose consultation, concurrent review, proctoring, or other conditions or restrictions on the assigned duties of the involved party in order to reduce the substantial likelihood of violation of standards of conduct.

X. Auditing and Monitoring

The Chief Compliance and Risk Officer will conduct ongoing evaluations of compliance and risk management processes involving thorough monitoring and regular reporting to the officers of the Organization.

The Chief Compliance and Risk Officer will develop an annual audit plan that is designed to address the Organization's key compliance, clinical, and patient safety-related risks, including but not limited to laws governing kickback arrangements, physician self-referral prohibition, CPT and ICD coding and billing, claim development and submission, reimbursement, reporting, quality assurance and quality improvement, and record-keeping. The Pharmacy will have a Quality Assurance program in place to monitor medication errors and drug interactions. Reversed claims for unclaimed filled prescriptions will be tracked to ensure appropriate billing.

The audit work program steps will inquire into compliance with specific rules and policies that have been the focus of Medicaid and Medicare fiscal intermediaries or carriers as evidenced by the Medicare Fraud Alerts, OIG audits and work plans, OMIG audits and work plans and evaluations and publicly announced law enforcement initiatives. Audits should also reflect areas of concern that are specific to the Organization, including results of all internal or external audits, including audits conducted by State or Federal government. Also, the audit program will identify and manage risks by actively and systematically spotting, preventing, and addressing potential patient safety issues. By integrating risk management

with quality improvement and compliance activities, Trillium not only promotes best clinical practices and enhances patient experiences but also reduces the likelihood of future problems.

The design, implementation, and results of any internal or external audit are documented, and the results are shared with the compliance and risk management committee and governing body. The Chief Compliance and Risk Officer should be aware of patterns and trends in deviations identified by the audit that may indicate a systemic problem.

A. ANNUAL COMPLIANCE AND RISK MANAGEMENT PROGRAM REVIEW

The organization has a process for reviewing at least annually to determine the effectiveness of its compliance and risk management program and whether any revision or corrective action is required.

The review may be carried out by the Chief Compliance and Risk Officer, Compliance and Risk Management Committee, external auditors or other designated staff with the necessary knowledge and expertise to evaluate the effectiveness of the components of the program and are independent from the functions being reviewed.

The review may include on-site visits, interviews with affected individuals, review of records, surveys or any other comparable method that the organization deems appropriate, provided the method does not compromise the independence or integrity of the review.

The organization shall document the design, implementation and results of the effectiveness review and share the results with the chief executive officer, senior management, the compliance and risk management committee, and the board of directors.

B. EXCLUDED PROVIDERS

The organization will confirm the identity and determine the exclusion status of all affected individuals. In determining the exclusion status, the organization shall review the following State and Federal databases prior to hiring or contracting and at least every 30 days thereafter:

D. NYS Office of the Medicaid Inspector General Exclusion List
E. Health and Human Services Office of the Inspector General's List of Excluded Individuals and Entities.

The results of the screening activity are promptly shared with the appropriate personnel.

XI. Responding to Detected Offenses and Developing Corrective Action Initiatives

Violations of the Organization's compliance and risk management program, failure to comply with applicable state or federal law, and other requirements of government and private health plans, and other types of misconduct may threaten the Organization's status as a reliable, honest, and trustworthy provider, capable of participating in federal healthcare programs. Detected, but uncorrected, misconduct may seriously endanger the mission, reputation, and legal status of the Organization. Consequently, upon reports or reasonable indications of suspected noncompliance, the Chief Compliance and Risk Officer must initiate an investigation to determine whether a material violation of applicable laws or requirements has occurred.

INVESTIGATION REQUIREMENTS

The organization shall take prompt action to investigate the conduct in question and determine what if any corrective action is required and promptly implement such corrective action.

The steps in the internal investigation may include interviews and a review of relevant documentation. The organization will maintain:

A. Records of the investigation shall contain:

B. Documentation of the alleged violation,

C. A description of the investigative process,

D. Copies of interview notes and key documents,

E. A log of witnesses interviewed, and

F. The documents reviewed,

G. Results of the investigation,

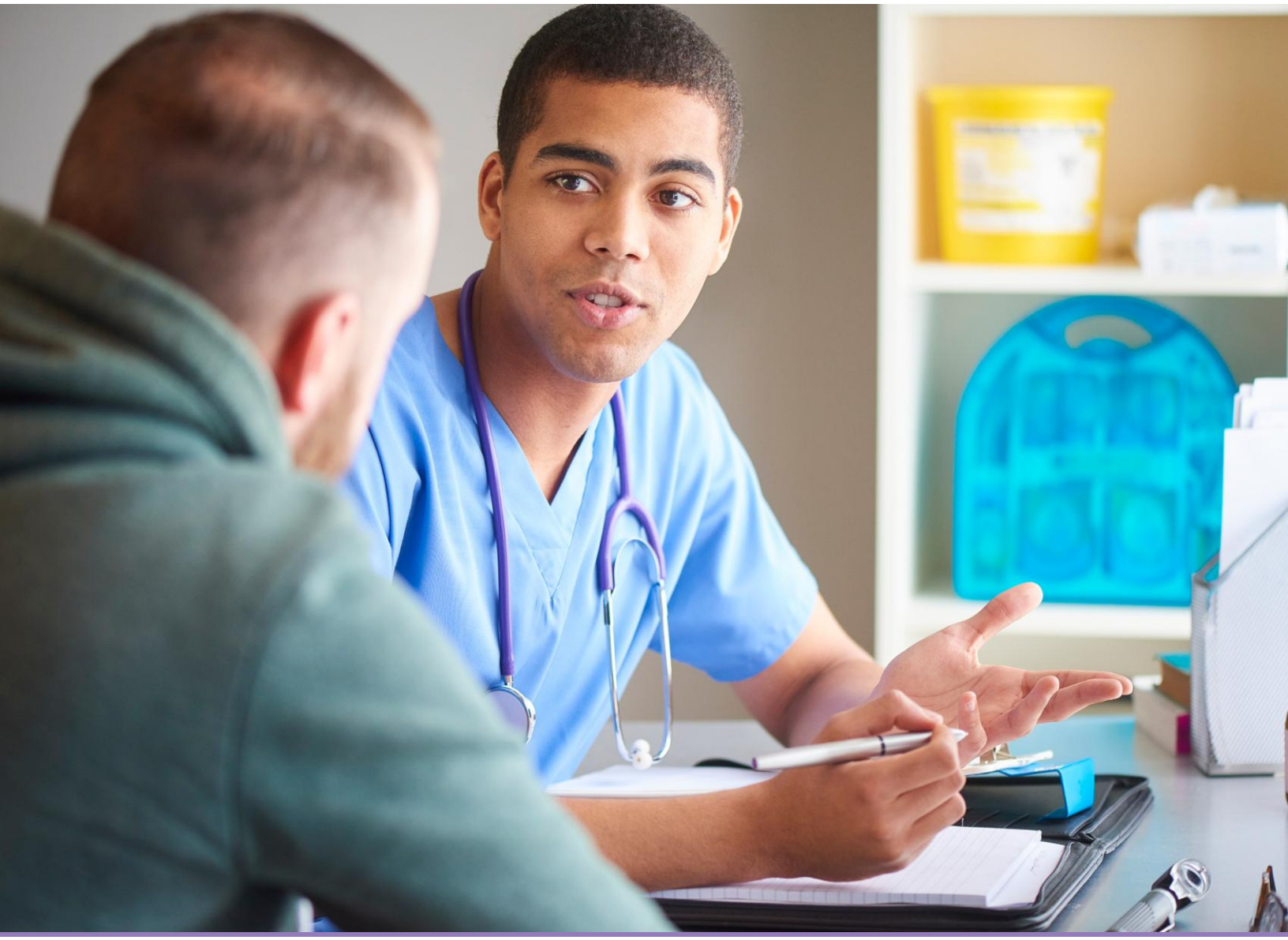
H. Corrective actions implemented and

I. Any disciplinary action taken.

If an investigation of an alleged violation is undertaken, and the Chief Compliance and Risk Officer believes the integrity of the investigation may be hampered by the presence of employees under investigation, those employees should be removed from their current work activities pending completion of that portion of the investigation. These employees will be temporarily suspended with pay pending the outcome of the investigation.

Additionally, the Chief Compliance and Risk Officer must take appropriate steps to secure or prevent the destruction of documents or other evidence relevant to the investigation.

If the results of the internal investigation identify a problem, the response may be immediate referral to criminal and/or civil law enforcement authorities, development of a corrective action plan, a report to the government, and submission of any overpayments, if applicable. If potential fraud or violations of the False Claims Act are involved, the Chief Compliance and Risk Officer should promptly report the potential violation to the Office of the Inspector General or the Department of Justice, or other appropriate governmental entity where such reporting is otherwise required by law, rule, or regulation.



XII. OMIG Self-Disclosure Program

Any person who has received an overpayment under the program, either directly or indirectly shall report, return and explain the overpayment by submission of a Self-Disclosure Statement to OMIG's Self-Disclosure Program.

DEADLINE:

The person shall report and return the overpayment and interest, if applicable to the department and explain the reasons for the overpayment to OMIG by the later of:

- The date which is sixty (60) days after the date on which the overpayment was identified or
- The date of any corresponding cost report is due, if applicable.

A person has identified an overpayment when that person has or should have, through the exercise of reasonable due diligence, determined that they have received an overpayment and quantified the amount of the overpayment.

When a person fails to exercise reasonable due diligence, and the person in fact receives an overpayment, they shall be subject to any enforcement action authorized by section 521-3.7 of this subpart of the Social Services Law and any applicable provisions of federal and state law including but not limited to Article XIII of the NYS Finance Law.

When making a repayment for an overpayment, the Organization should follow the direction from OMIG following the self-disclosure to inform the payer of the following: (1) the refund is being made pursuant to a voluntary compliance program; (2) a description of the complete circumstances prompting the overpayment; (3) the methodology by which the overpayment was determined; (4) any claim-specific information used to determine the overpayment; and (5) the amount of the overpayment.

The President, CEO of the Organization shall have the authority and responsibility to direct repayment to payers and the reporting of misconduct to enforcement authorities as is determined, in consultation with legal counsel, to be appropriate or required by applicable laws and rules.

If the President, CEO of the Organization discovers credible evidence of misconduct, and has reason to believe that the misconduct may violate criminal, civil, or administrative law, then the Chief Compliance and Risk Officer will promptly report the matter to the appropriate government authority within a reasonable time frame, but not more than 60 days after determining that there is credible evidence of a violation.

When reporting misconduct to the government, the Chief Compliance and Risk Officer should provide all evidence relevant to the potential violation of applicable federal or state laws and the potential cost impact.

XIII. Trillium's Code of Conduct

CODE OF CONDUCT

The Organization is committed to the highest standards of business ethics and integrity as well as compliance with the laws and regulations governing our business. We place the utmost importance on the observance of our Code of Conduct, and all Employee, Board Members, and Contractors are expected to comply with the Organization's Code of Conduct, Compliance and Risk Management Plan, Organization policies, and applicable laws and regulations related to their job function.

Employees, Board Members, and Contractors also have a duty to report any potential or actual violation of the Organization's Code of Conduct, Compliance and Risk Management Plan, policy, or applicable law or regulation. At Trillium, we strive to create a culture of compliance and quality services. Employees, Board Members, and Contractors are expected to "do the right thing" when performing their job function for the Organization. We must conduct our business with integrity and professionalism and exercise good judgment and ethical conduct.

A. STANDARDS OF CONDUCT

The Organization's Affected Individuals are bound to comply, in all official acts and duties, with all applicable laws, rules, regulations, and standards of conduct, including, but not limited to laws, rules, regulations, and directives of the federal government and the state of New York, in addition to rules and policies and procedures of the Organization. These current and future standards of conduct are incorporated by reference in this Compliance and Risk Management Plan.

All candidates for employment shall undergo a reasonable and prudent background investigation, including a reference and criminal background check. Due diligence will be used in the recruitment and hiring process to prevent the appointment to positions with substantial discretionary authority, persons whose record (professional licensure, credentials, prior employment, criminal record
or specific "exclusion" from Medicaid-funded programs) gives reasonable cause to believe the individual has a propensity to fail to adhere to applicable standards of conduct.

All new employees will receive orientation and training in compliance and risk management policies and procedures. Participation in required training is a condition of employment. Failure to participate in required training may result in disciplinary actions, up to and including termination of employment.

Every employee is asked to sign a statement certifying they have received, read, and understood the contents of the compliance and risk management plan.

Every employee will receive an initial compliance and risk management orientation and periodic training updates in compliance and risk management protocols as they relate to the employee's individual duties.

Non-compliance with the plan or violations will result in sanctioning of the Affected Individual involved in accordance with Section IX Disciplinary Standards.

B. PATIENT/CLIENT RIGHTS

We treat our patients/clients with respect and dignity and provide care that is both necessary and appropriate. No distinction is made in the admission, transfer, discharge or care of individuals on the basis of race, creed, religion, national origin, gender, source of payment, or disability. Clinical care is provided based on identified healthcare needs, and Case Management is provided based on needs identified through a uniform assessment tool, not on financial criteria, and no treatment or action is undertaken without the informed consent of the patient or an authorized representative. Patients/clients are provided with a written statement of rights which conforms to all applicable laws, and their autonomy and privacy are respected within the context of a safe congregate setting.

Employees involved in patient/client care are expected to know and comply with all applicable laws and regulations and our policies and procedures governing their particular program.

C. PERSONAL HEALTH INFORMATION/HIPAA/ARTICLE 27-F COMPLIANCE

The Organization collects personal health information about our patients/clients to provide the best possible care. We realize the sensitive nature of this information and are committed to safeguarding patients'/clients' privacy.

The Organization has created the Privacy Officer position in accordance with the HIPAA Privacy Rule. The Privacy Officer is responsible for the development and implementation of policies, procedures and educational programs that will ensure that the Organization will continue to be compliant with the Privacy regulations and will also ensure that protected health information is secure.

In order to ensure that confidentiality is maintained, employees and their representatives must adhere to the following rules:

- Do not discuss protected health information (PHI)/ client information in public areas such as elevators, hallways, common gathering areas.
- Limit release of PHI/client information to the minimum reasonably necessary for the purpose of the disclosure.
- Do not disclose PHI without an appropriate consent signed by the patient/client unless it is related to the person's care, payment of care, or health care operations of the Organization. In an emergency situation, a patient's consent may not be required when a healthcare provider treating the patient requests information, but the name and
- affiliation of the person requesting the information must be confirmed and documented in the medical record.
- Honor any restrictions on uses or disclosure of information placed by the patient/client.
- Make sure PHI/client information stored in the computer system is properly secured.
- Be familiar with and comply with special confidentiality rules governing the disclosure of HIV/AIDS, alcohol, substance abuse, and mental health treatment.

The Organization has created and maintains the Privacy Officer position in accordance with the HIPAA Privacy Rule. The Privacy Officer is responsible for:

- Managing the Organization's privacy policies, procedures, and data governance
- Driving privacy-related awareness and training among employees
- Leading incident response, including data breach preparedness
- Communicating privacy goals and values both internally and externally
- Designing controls for managing privacy compliance
- Assessing privacy-related risks arising from existing services
- Conducting Privacy Risk Assessments to identify risks in new or changed business activities
- Monitoring the effectiveness of privacy-related risk mitigation and compliance measures

Additionally, the Organization has created and maintains a Security Officer position in accordance with the HIPAA Security Rule. The Security Officer is responsible for the development and implementation of the policies and procedures required by the Security Rule.

The Security Officer is responsible for ensuring Trillium engages in the following activities:

- Maintain appropriate security measures to ensure the confidentiality, integrity and availability of patients' electronic protected health information (EPHI).
- Adhere to applicable federal and state security laws and standards.
- Provide security training and orientation to all employees, volunteers, medical and professional staff.
- Comply with Security Policies, including periodic risk assessments.
- Monitor access controls to EPHI to ensure appropriate access to authorized personnel.
- Maintain hardware and software with the appropriate patches and updates.
- Maintain a validation of compliance with the Payment Card Industry Data Security Standards, a set of security controls that businesses are required to implement to protect credit card data

D. MEDICAL NECESSITY

The Organization will take reasonable measures to ensure that only claims for services that are reasonable and necessary, given the patient's condition/client's needs are billed.

Documentation will support the determinations of medical necessity/client need when providing services.

The Organization is aware that private and governmental third-party payers will only pay for tests that meet the coverage criteria and are reasonable and necessary to treat or diagnose a patient. Therefore, the Organization's Providers will use prudent ordering practices.

In requesting diagnostic procedures or tests, the Organization's Providers will make an independent medical necessity decision with regard to each item ordered. A diagnosis will be submitted for all tests ordered. Documentation of findings and diagnoses will support the medical necessity of the service.

The Organization's Providers understand that private and governmental third-party payers generally have limitations on laboratory and diagnostic tests; therefore, the prior authorization process will be followed.

The Organization's providers will order tests or services that are medically necessary for the appropriate treatment of the patient.

E. BILLING

All claims for services submitted to private and governmental third-party payers or other health benefits programs will correctly identify the services ordered. Only those tests ordered by an authorized Provider that are performed and that meet private and governmental third-party payer's criteria will be billed.

Intentionally or knowingly up-coding (the selection of a code to maximize reimbursement when such code is not the most appropriate descriptor of the service offered) may result in immediate termination. The Organization's providers must provide documentation to support the current CPT and ICD codes used based on medical findings and diagnoses.

Immediate disciplinary action, up to and including termination, will be implemented for instances of intentional misrepresentation of any service provided that results in over-billing.

All individuals who provide billing information and billing department employees who prepare or submit billing statements must comply with all applicable laws, rules, and regulations and the Organization's policies.

The Organization will promptly return to payers any payments that we determine do not conform to our policies and applicable laws in accordance with the OMIG (above) or OIG Self-Disclosure Protocols as applicable.

As healthcare/human service Providers, our business involves reimbursement under government programs, which require the submission of certain reports of our costs of operations. The Organization complies with all federal and state laws and regulations relating to cost reports, which define what costs are allowable and describe the appropriate methodologies to claim reimbursement for the cost of services provided to program beneficiaries. Given the complexity of this area, all issues related to the completion and settlement of cost reports must be communicated through or coordinated with the Chief Financial Officer as well as the Chief Compliance and Risk Officer.

F. COMPLIANCE WITH APPLICABLE HHS FRAUD ALERTS

The Chief Compliance and Risk Officer will review the Medicaid/Medicare Fraud Alerts.

The Chief Compliance and Risk Officer will ensure that any conduct disparaged by Fraud Alert is immediately ceased, implement corrective actions, and take reasonable actions to ensure that future violations do not occur.

G. ANTI-KICKBACK/INDUCEMENTS

The Organization will not participate in nor condone the provision of inducements or receipt of kickbacks to gain business or influence referrals. The Organization's Providers will consider the patient/client's interests in offering referral for treatment, diagnostic, or service options.

Federal and state laws prohibit any form of kickback, bribe, or rebate, either directly or indirectly, in cash or in kind, to induce the purchase or referral of goods, services, or items paid for by Medicare or Medicaid.

Self-referral laws prohibit a Provider from referring a patient for certain types of health services to an entity with which the provider or members of his or her immediate family has a financial relationship, unless there is an applicable exception under the self-referral law.

Since violations of these laws may subject both the Organization and the individual involved to civil and criminal penalties and exclusion from government-funded healthcare programs, all proposed transactions with healthcare providers must be reviewed with legal counsel.

Any employee involved in promoting or accepting kickbacks or offering inducements may be terminated immediately.

H. RELATIONSHIPS WITH VENDORS AND SUPPLIERS

The Organization is committed to employing the highest ethical standards in its relationships with vendors and suppliers with respect to source selection, negotiation, determination of contract awards, and administration of purchasing activities. All vendors and suppliers are to be selected solely on the basis of objective criteria; personal relationships and friendships play no part in

the selection process. The Organization's vendors are screened on a monthly basis to ensure they are not on any federal or state exclusion list. Any vendor or supplier who has access to the Organization's PHI and is not a covered entity will be required to enter into a Business Associate

Agreement to comply with applicable federal and state confidentiality and data protection rules, including HIPAA and 42 C.F.R. Part 2, federal regulations that govern the confidentiality of drug and alcohol abuse treatment and prevention records. The Organization will maintain a vendor review program for selecting and assessing the appropriate safeguards and security controls for key vendors.

I. RETENTION OF RECORDS/DOCUMENTATION/DESTRUCTION

The Organization will ensure that all records required by federal and/or state law are created and maintained. All records will be maintained for a period of no less than seven (7) years. Records are available to the compliance and risk management department, OMIG, MFCU, and other appropriate federal and state agencies upon request, copies of such records.

Documentation of compliance and risk management efforts will include staff meeting and committee minutes, audit reports, memoranda concerning compliance and risk management protocols, problems identified and corrective actions taken, the results of any investigations, and documentation supportive of assessment findings, diagnoses, treatments, and plan of care.

Hard copy data that is not necessary or which the Organization is no longer required to retain will be sent to a professional shredding company, where the data will be shredded using a cross-cut shredder to effect 5/16 inch wide or smaller strips. Media containing sensitive data will be sanitized in a manner that is consistent with the standards set forth in the National Institute of Science and Technology Special Publication 800-88 rev. 1, Guidelines for Media Sanitation.

J. MEDICAL RECORD DOCUMENTATION

Timely, accurate, and complete documentation is important to clinical patient care. This documentation not only facilitates high-quality patient care, but also serves to verify that billing is accurate as submitted.

The Organization requires that providers meet the following documentation guidelines:

- The medical record/client record is complete and organized.
- Documentation is timely.
- The documentation of each patient encounter includes the reason for the encounter, any relevant history, physical examination findings, prior diagnostic test results, assessment, clinical impression or diagnosis, plan of care, date and legible identity of the observer.
- CPT and ICD-10 codes used for claims submission are supported by documentation in the medical record.
- Appropriate health risk factors are identified. The patient's progress, his, her, or their response to treatment.
- Care management encounters will be documented per New York State Department of Health guidelines.

The Organization will maintain a process for identifying and reviewing its billing and coding to ensure compliance with applicable state and federal requirements.

K. PRESCRIPTION DRUGS AND CONTROLLED SUBSTANCES

The Organization's employees routinely have access to prescription drugs, controlled substances and other medical supplies. In accordance with federal, state, and local laws, it is strictly prohibited to divert prescription drugs and controlled substances to unauthorized individuals, to administer them without proper orders, to distribute adulterated, misbranded, mislabeled or expired drugs or devices, or to fail to report significant adverse events. Any employee of the Organization who becomes aware of a potential lapse in security or the improper diversion of drugs must report the incident immediately to his/her/their supervisor or the Chief Compliance and Risk Officer.

L. PERSONAL CONDUCT AND BUSINESS ETHICS

GIFTS AND GRATUITIES: The Organization's employees cannot accept money, gifts, services, entertainment or other items of value which may influence your actions or decisions. The Organization has policies on gifts and gratuities and vendor interaction that you must follow.

DISCRIMINATION: The Organization practices fair and equal treatment of employees, volunteers, patients, families and others by celebrating the diversity of all people, without discrimination on the basis of race, color, national origin, alienage, citizenship, religion, creed, gender, pregnancy, age, physical or mental disability, marital or partnership status, or expression of any other characteristic protected by law. You are expected to abide by the Standards of this Code, including reporting discrimination, intimidation, or violence of any kind that you witness in the workplace.

HARASSMENT/SEXUAL HARASSMENT: Workplace harassment, sexual harassment, comments, or other conduct that creates an intimidating or offensive environment will not be tolerated. The Organization has adopted policies with respect to workplace and sexual harassment that provide a way for you to bring such improper conduct to the attention of management.

STEWARDSHIP: We safeguard the Organization's assets, including medical records, equipment, supplies, financial data, funds, employee sensitive data, intellectual property rights, research data, business strategies, and plans about the Organization's activities, and not use these assets for personal gain.

CLINICAL RESEARCH: Ethics and integrity are essential to the advancement of scientific knowledge. The Organization is committed to conducting research in accordance with professional, ethical and legal standards. All patients who are asked and/or choose to participate in a research study are advised of all alternative treatments available to them along with the risks and benefits of the proposed treatments. It is essential that our patients are making informed decisions with respect to research studies.

WORKPLACE VIOLENCE: The Organization is committed to maintaining a workplace that is free from acts and threats of violence. The Organization has a workplace violence prevention program to protect colleagues, patients, visitors, property or other persons against violence or threats of violence while on its premises. Although some incidents of violence are beyond our control, we believe we can help prevent or minimize them with the cooperation of all colleagues. Early reporting and response in these situations can improve the work environment and prevent escalation.

WEAPONS: We are a weapons-free organization to ensure a safe and secure environment. The Organization has processes on how to report and respond to situations where a colleague encounters a weapon in the workplace.

CONTROLLED SUBSTANCES: Unauthorized access, use or diversion (e.g. theft) of controlled substances is prohibited. Immediately report to your manager or appropriate department any potential issues or concerns you identify involving the security or diversion of controlled substances.

FITNESS AND DRUG-FREE ENVIRONMENT OF CARE: The Organization works diligently to maintain an alcohol-free and drug-free environment across our continuum of care. Our employees and contractors are expected to perform all job duties and responsibilities in a professional manner, free from the influence of alcohol, drugs or other substances which may impair our job performance or judgment. If it is suspected that an employee or contractor is under the influence of drugs or alcohol while at work, appropriate drug or alcohol testing may be required. Likewise, any unlawful manufacture, sale, distribution, or possession of any illegal substance on any of the Organization's locations will not be tolerated. Any employee or contractor found to be performing any activity for the Organization while impaired by or under the influence of alcohol or illegal drugs will be subject to disciplinary action up to and including termination of employment.

MANAGEMENT OF DONATED FUNDS: The Organization, and its associated foundation, as non-profit organizations, are being supported by individual, foundation, and corporate donors. We have been entrusted with these funds to achieve our mission and we take our duty to use these funds carefully and to meet our responsibilities to donors very seriously. We adhere to the highest standards in the solicitation, acceptance, recording and use of donated funds

XIV. Response to City, State, or Federal Law Enforcement Officer or Agent Visits

IN THE EVENT THAT CITY, STATE, AND/OR FEDERAL LAW ENFORCEMENT OFFICERS OR AGENTS, INCLUDING LOCAL POLICE, STATE TROOPERS, FBI, DOJ, OR ICE VISIT THE ORGANIZATION FOR THE PURPOSE OF:

- Arrests
- Civil Apprehensions
- Searches
- Inspections
- Seizures
- Service of charging documents or subpoenas
- Interviews
- Immigration enforcement surveillance

THE ORGANIZATION REQUIRES THAT STAFF RESPOND ACCORDING TO THE FOLLOWING GUIDANCE:

- Stay calm and professional and avoid confrontation or escalation
- Request identification
- Ask them to wait in the lobby or waiting areas
- Notify leadership immediately; contact either the Chief Compliance and Risk Officer, or the Director of Compliance, Privacy, and Risk. If either of them is unavailable, contact another ELT member
- Do not provide information
- Avoid answering questions without authroization

XV. Risk Management Plan

A. PURPOSE

Trillium's Risk Management Plan is designed to support the mission and vision of Trillium Health as it pertains to clinical risk and patient safety. It addresses visitor, third-party, volunteer, and employee safety as well as potential business, operational, and property risks.

B. DEFINITIONS

ADVERSE EVENT OR INCIDENT: An undesired outcome or occurrence, not expected within the normal course of care or treatment, disease process, condition of the patient, or delivery of services.

CLAIMS MANAGEMENT: Activities undertaken by the risk manager to exert control over potential or filed claims against the organization or its providers. These activities include identifying potential claims early, notifying the organization's liability insurance carrier or defense counsel of potential claims and lawsuits, evaluating liability and associated costs, identifying and mitigating potential damages, assisting with the defense of claims by scheduling individuals for deposition, providing documents or answers to written interrogatories, implementing alternate dispute-resolution tactics, and investigating adverse events or incidents.

ENTERPRISE RISK MANAGEMENT (ERM): "Enterprise risk management in healthcare promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connections to total value." (ASHRM, 2012) ERM is further defined by RMIS (the risk management society™) as a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio. ERM represents a significant evolution beyond previous approaches to risk management. ERM does the following:

a) Encompasses all areas of organizational exposure to risk (e.g., financial, operational, reporting, compliance, governance, strategic, reputational)

b) Prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual "silos"

c) Evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders

d) Recognizes that individual risks across the organization are interrelated and can create a combined exposure that differs from the sum of the individual risks

e) Provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature

f) Views the effective management of risk as a competitive advantage

g) Seeks to embed risk management as a component in all critical decisions throughout the organization

FAILURE MODE AND EFFECTS ANALYSIS: A proactive method for evaluating a process to identify where and how it might fail and for assessing the relative impact of different failures in order to identify the parts of the process that are most in need of improvement.

HAZARDS: Situations with the potential to cause harm.

LOSS CONTROL/LOSS REDUCTION: The minimization of the severity of losses through methods such as claims investigation and administration, early identification and management of events, and minimization of potential loss of reputation.

LOSS PREVENTION: The minimization of the likelihood (probability) of a loss through proactive methods such as risk assessment and identification; staff and volunteer education, credentialing, and development; policy and procedure implementation, review, and revision; preventive maintenance; quality/performance review and improvement; root-cause analysis; and others.

NEAR MISS: An event or situation that could have resulted in an accident, injury, or illness but did not, either by chance or through timely intervention (e.g., a procedure almost performed on the wrong patient owing to a lapse in verification of patient identification but caught at the last minute by chance). Near misses are opportunities for learning and afford the chance to develop preventive strategies and actions. Near misses receive the same level of scrutiny as adverse events that result in actual injury.

PATIENT SAFETY GOALS: National Patient Safety Goals (NPSGs) for ambulatory care, established by the Joint Commission. The purpose of NPSGs is to improve patient safety by focusing on problems in healthcare safety and how to solve them.

POTENTIALLY COMPENSABLE EVENT (PCE): An unusual occurrence or serious injury for which there is neither an active claim nor institution of formal legal action but that, in the organization's judgment, is reportable to the party (or parties) providing the medical malpractice insurance. Examples include delay or failure in diagnosing a patient's condition, an adverse reaction to treatment, significant complaints from a patient or family regarding care or treatment (actual or perceived), and an attorney request for medical records, among others.

RISKS: The probability that a specific adverse event will occur in a specific time period or as a result of a specific situation**.**

RISK ANALYSIS: Determination of the causes, potential probability, and potential harm associated with an identified risk and alternatives for addressing the risk. Examples of risk analysis techniques include failure mode and effects analysis, systems analysis, root-cause analysis, and tracking and trending of adverse events and near misses.

RISK ASSESSMENT: Activities undertaken in order to identify potential risks and unsafe conditions inherent in the organization or within targeted systems or processes. By conducting a risk assessment, organizations capture feedback on issues that may affect quality of care, efficiency, or costs. Examples of tools utilized include risk matrices, structured surveys, quality measures, and review of patient complaints to identify issues.

RISK AVOIDANCE: The risk assessment technique that entails eliminating hazards, activities, and exposures that place an organization's valuable assets (patients) at risk. Examples include protective safeguards (through policy, training, or technology), the informed consent process, and compliance with regulations.

RISK CONTROL: Treatment of risk using methods aimed at eliminating or lowering the probability of an adverse event (e.g., loss prevention through a falls prevention program, procuring bariatric chairs [for waiting rooms and exam areas] to accommodate obese or overweight patients); eliminating, reducing, or minimizing harm to individuals; and minimizing the financial severity of losses when they occur (e.g., loss reduction through patient follow-up regarding abnormal lab results).

RISK FINANCING: Financing strategies, including all the ways of generating funds to pay for losses that risk control techniques do not entirely prevent. These treatment techniques include risk retention and risk transfer. They involve analysis of the costs associated with quantifying risk and funding for it, such as through general liability insurance.

RISK IDENTIFICATION: The process used to identify situations, policies, or practices that could result in the risk of patient harm or financial loss. Sources of information include proactive risk assessments, closed claims data, adverse event reports, past accreditation or licensing surveys, medical records, clinical and risk management research, walk-through inspections, safety and quality improvement committee reports, insurance company claim reports, risk analysis methods such as failure mode and effects analysis and systems analysis, and informal communication with healthcare providers.

RISK MANAGEMENT: Clinical and administrative activities undertaken to identify, evaluate, prevent, and control the risk of injury to patients, staff, visitors, volunteers, and others and to reduce the risk of loss to the organization itself. Activities include the process of making and carrying out decisions that will prevent or minimize clinical, business, and operational risks.

DATA, INFORMATICS, SYSTEM & QUALITY (DISQ): The Trillium department that is responsible for data collection and processing, information analysis, and the generation of statistical trend reports for the identification and monitoring of events, claims, finances, and more.

RISK RETENTION: Internally driven financing mechanisms (e.g., self-insured retentions) intended to pay for accidental and uninsurable losses.

RISK TRANSFER: Techniques involving the process of shifting the financial burden of losses to an external party or parties (e.g., insurance, contracts).

ROOT-CAUSE ANALYSIS: A process for identifying the basic or causal factor(s) that underlie the occurrence or possible occurrence of an adverse event. This problem-solving method is used for identifying the root causes of faults or problems. A factor is considered a root cause if its removal from the problem-fault-sequence prevents the final undesirable event from recurring; whereas a causal factor is one that affects an event’s outcome, but is not a root cause.

SENTINEL EVENT: Defined by the Joint Commission as an unexpected occurrence involving death or serious physical or psychological injury, or the risk thereof. Serious injury specifically includes loss of limb or function. The phrase “or the risk thereof” includes any process variation for which a recurrence would carry a significant chance of a serious adverse event.

TRIGGER METHODOLOGY: A method of measuring harm related to the occurrence of adverse events**.** The method utilizes a clearly defined list of patient events (also known as a "trigger tool") against which patient medical records are screened. Screening criteria are based on high-risk areas, or areas identified as "red flags" through event reporting or as a result of a severe adverse event (e.g., new diagnosis of cancer, use of more than five medications, high-risk pregnancy).

UNSAFE OR HAZARDOUS CONDITION: Any set of circumstances (exclusive of a patient's own disease process or condition) that significantly increases the likelihood of a serious adverse outcome for a patient or likelihood of a loss due to an accident or injury to a visitor, employee, volunteer, or other individual.

C. GUIDING PRINCIPLES

The Risk Management Plan is an overarching, conceptual framework that guides the development of a program for risk management and patient safety initiatives and activities. The plan is operationalized through a formal, written risk management and patient safety program. This document serves as a formal, written plan for the risk management and patient safety program.

The Patient Safety and Risk Management Program supports the Trillium Health philosophy that patient safety and risk management are everyone's responsibility. Teamwork and participation among management, providers, volunteers, and staff are essential for an efficient and effective patient safety and risk management program. All staff are key to the successful implementation of the risk management program and are expected to be knowledgeable about and participate in risk management activities; to assist with the implementation of recommended improvements; and to identify risk events and opportunities for improvement. The program will be implemented through the coordination of multiple organizational functions and the activities of multiple staff members.

Trillium supports the establishment of a just culture that emphasizes implementing evidence-based best practices, learning from error analysis, and providing constructive feedback rather than blame and punishment. In a just culture, unsafe conditions and hazards are readily and proactively identified, medical or patient care errors are reported and analyzed, mistakes are openly discussed, and suggestions for systemic improvements are welcomed. Individuals are still held accountable for compliance with patient safety and risk management practices. As such, if evaluation and investigation of an error or event reveal reckless behavior or willful violation of policies, disciplinary actions can be taken.

The Trillium Health Risk Management Plan stimulates the development, review, and revision of the organization's practices and protocols in light of identified risks and chosen loss prevention and reduction strategies. Principles of the Plan provide the foundation for developing key policies and procedures for risk management activities, including the following:

a) Claims and insurance management

b) Complaint resolution

c) Confidentiality and release of information

d) Compliance efforts

e) Safe and secure use of technology

f) Event investigation, root-cause analysis, and follow-up

g) Proactive analyses (e.g., failure mode and effects analysis, proactive risk assessments)

h) Provider and staff education (including such items as documentation practices and effective tracking)

i) Competency validation, credentialing and privileging requirements, and background checks

j) Systems for monitoring and tracking referrals (specialty care, hospital, and or emergency department admissions) and diagnostic laboratory values and other tests

k) Reporting and management of adverse events and near misses

l) Trend analysis of events, near misses, and claims

m) Implementing performance improvement strategies to mitigate risk

D. LEADERSHIP

The success of the Trillium Health Risk Management Program requires top-level commitment and support. The governing board or designee authorizes the formal program and adoption of this Plan as noted by their signature.

The governing board and senior executives are committed to promoting the safety of all patients, visitors, employees, volunteers, and other individuals involved in operations of the organization. Trillium's Risk Management Program is designed to reduce system-related errors and potentially unsafe conditions by implementing continuous improvement strategies to support an organizational culture of safety.

E. PROGRAM GOALS AND OBJECTIVES

Trillium's Management Program goals and objectives include the following:

a) Continuously improve patient safety and minimize or prevent the occurrence of errors, events, and system breakdowns leading to harm of patients, staff, volunteers, visitors, and others through proactive risk management and patient safety activities

b) Minimize adverse effects of errors, events, and system breakdowns when they do occur

c) Minimize losses to the organization overall by proactively identifying, analyzing, preventing, and controlling potential clinical, business, financial, and operational risks

d) Facilitate compliance with regulatory, legal, and accrediting agency requirements (e.g., Patient-Centered Medical Home, *The Joint Commission, Accreditation Association of Ambulatory Health Care*)

e) Protect human and intangible resources (e.g., reputation)

F. SCOPE AND FUNCTIONS OF THE PROGRAM

The Trillium Risk Management Program interfaces with many operational departments and services throughout the health center, as well as HRSA.

FUNCTIONAL INTERFACES

Functional interfaces with the patient safety and risk management program include areas such as credentialing and privileging, information technology, event reporting and investigation, performance assessment and improvement, volunteers, infection control, and administration. All areas work together on risk reduction strategies and methods as defined in this plan.

G. RISK MANAGEMENT PROGRAM FUNCTIONS

Risk management functional responsibilities include the following:

a) Developing systems for and overseeing the reporting of adverse events, near misses, and potentially unsafe conditions. Reporting responsibilities may include internal reporting as well as external reporting to regulatory, governmental, or voluntary agencies. This includes the development and implementation of event reporting policies and procedures.

b) Ensuring the collection and analysis of data to monitor the performance of processes that involve risk or that may result in serious adverse events, near misses, and potentially unsafe conditions; providing feedback to providers and staff; and using this data to facilitate systems improvements to reduce the probability of occurrence of future related events (e.g., preventive screening, diagnostic testing, medication use processes, perinatal care). Risk assessment tools include the use of failure mode and effects analysis, system analysis, root-cause analysis, and other tools.

c) Working closely with the organizational Data, Informatics, Strategy & Quality (DISQ) for data collection and processing, information analysis, and generation of statistical trend reports for the identification and monitoring of adverse events, claims, finances, and effectiveness of the risk management program. This system may utilize and include, but is not limited to, attorney requests for medical records, x-rays, laboratory reports; event reports; medical record reviews; patient complaints; and results of failure mode and effects analysis of high-risk processes, as well as root-cause analyses of sentinel events.

d) Ensuring compliance with data collection and reporting requirements of governmental, regulatory, and accrediting agencies.

e) Facilitating and ensuring the implementation of patient safety initiatives such as improved tracking systems for preventive screenings and diagnostic tests, medication safety systems, and falls prevention programs.

f) Facilitating and ensuring provider and staff participation in educational programs on patient safety and risk management.

g) Facilitating a culture of safety in the organization that embodies an atmosphere of mutual trust in which all providers and staff members can talk freely about safety problems and potential solutions without fear of retribution. This ordinarily involves performing safety culture surveys and assessments.

h) Proactively advising the organization on strategies to reduce unsafe situations and improve the overall environmental safety of patients, visitors, staff, and volunteers.

i) Preventing and minimizing the risk of liability to the health center, and protecting the financial, human, and other tangible and intangible assets of the health center.

j) Decreasing the likelihood of claims and lawsuits by developing a patient and family communication and education plan. This includes communicating and disclosing errors and events that occur in the course of patient care with a plan to manage any adverse effects or complications.

k) Investigating and assisting in claim resolution to minimize financial exposure in coordination with the liability insurer and its representatives.

l) Reporting claims and potentially compensable events (PCEs) to the appropriate entity, including medical malpractice insurance providers or U.S. Department of Health and Human Services Federal Tort Claims Act (FTCA) claims (as appropriate) and other insurers in accordance with the requirements of the insurance policy/contract and FTCA requirements.

m) Supporting quality assessment and improvement programs throughout the organization.

n) Implementing programs that fulfill regulatory, legal, and accreditation requirements.

o) Establishing an ongoing Patient Safety/Risk Management Committee composed of representatives from key clinical and administrative departments and services.

p) Monitoring the effectiveness and performance of risk management and patient safety actions. Performance monitoring data may include the following:

q) Claims and claim trends, including:

- Culture of safety surveys
- Event trending data
- Ongoing risk assessment information
- Patient’s or family’s perceptions of how well the organization meets their needs and expectations
- Quality performance data
- Research data

r) Completing insurance and deeming applications.

s) Developing and monitoring effective handoff processes for continuity of patient care.

H. ADMINISTRATIVE AND COMMITTEE STRUCTURE AND MECHANISMS FOR COORDINATION

The Risk Management Program is administered through the Chief Compliance and Risk Officer or his designee. The Chief Compliance and Risk Officer reports to the chief executive officer (CEO). The Chief Compliance and Risk Officer interfaces with administration, staff, medical providers, and other professionals and has the authority to cross operational lines in order to meet the goals of the program. The Chief Compliance and Risk Officer (or alternate as designated) chairs the activities of the Compliance and Risk Management Committee**.** The committee meets regularly and includes representatives from key clinical and support services. The composition of the Compliance and Risk Management Committee is designed to facilitate the sharing of compliance and risk management knowledge and practices across multiple disciplines; to optimize the use of key findings from compliance and risk management activities in making recommendations; and to reduce the overall likelihood of adverse events and improve patient safety. The committee's activities are an integral part of a patient safety and quality improvement and evaluation system.

Documentation of the designation of the risk manager is contained in the Patient Safety/Risk Management Plan. The Chief Compliance and Risk Officer is responsible for overseeing day-to-day monitoring of patient safety and risk management activities and for investigating and reporting to the insurance carrier actual or potential clinical, operational, or business claims or lawsuits arising out of the organization, according to requirements specified in the insurance policy or contract. The Chief Compliance and Risk Officer serves as the primary contact between the organization and other external parties on all matters relative to risk identification, prevention, and control, as well as risk retention and risk transfer. The Chief Compliance and Risk Officer oversees the reporting of events to external organizations, per regulations and contracts, and communicates analysis and feedback of reported risk management and patient safety information to the organization for action.

I. REPORTING REQUIREMENTS, MONITORING, AND CONTINUOUS IMPROVEMENT

The Compliance and Risk Management Committee reviews risk management activities regularly. The Chief Compliance and Risk Officer reports activities and outcomes (e.g., claims activity, risk and safety assessment results, event report summaries, and trends) regularly to leadership and the governing board. This report informs them of efforts made to identify and reduce risks, reports on the success of these activities, and communicates outstanding issues that need input or support for action or resolution. Data reporting may include event trends, claims analysis, frequency and severity data, credentialing activity, relevant provider and staff education, and risk management/patient safety activities. In accordance with the organization's bylaws, recommendations from the Compliance and Risk Management Committee are submitted as needed to the board for approval. Performance improvement goals are developed to remain consistent with the stated risk management and patient safety goals and objectives. Documentation is in the form of compliance and risk management committee meeting minutes.

J. CONFIDENTIALITY

Any and all documents and records that are part of the patient safety and risk management process shall be privileged and confidential to the extent provided by state and federal law. Confidentiality protections may include attorney/client privilege, attorney work product, Patient Safety Organization, and peer review protections.

THE SIGNATURES BELOW REPRESENT AN ACCEPTANCE OF THE 2026 COMPLIANCE AND RISK MANAGEMENT PROGRAM.

SIGN:		**SIGN:**	
NAME:	GREGORY C. EWING,	**NAME:**	JASON BARENECUT-KEARNS
TITLE:	RISK MANAGER	**TITLE:**	PRESIDENT/CEO
DATE:		**DATE:**	
SIGN:		**SIGN:**	
NAME:	SARAH BOLDUC	**NAME:**	LESLIE CONNOLLY
TITLE:	CMO	**TITLE:**	BOARD CHAIR
DATE:		**DATE:**	

This Compliance and Risk Management Plan and Code of Conduct has attempted to provide the foundation for the development of an effective and cost-efficient compliance and risk management program.

This Compliance and Risk Management Plan and Code of Conduct may be altered or amended in writing only with the concurrence of the Compliance and Risk Management Committee of the Organization. The adoption of this Compliance and Risk Management Plan has been approved and authorized as designated below.

Trillium Health, Inc.

By: Gregory Ewing, SVP, Compliance, Privacy, Technology & Regulatory Affairs

Date: January 2026