Creating an Effective Compliance Plan

Community Behavioral Health

Creating an Effective Compliance Plan

- Introduction
- Compliance Risks
- Compliance Plan Structure: The 7 Elements
- Additional Resources

C·B·H

What is a compliance plan?

A compliance plan is a collection of internal policies and procedures designed to ensure that your organization adheres to the law. A well-crafted compliance plan can improve your organization's efficiency and the quality of care it provides and reduce costs.

Introduction:

What is a Compliance Plan, and Why is it Important?

Having a Compliance Plan is a CBH Requirement

As per the CBH Provider Manual
"Providers are reminded that the CBH Provider Agreement requires them to have a written Compliance Plan."

Please find the full Provider Manual At CBHPhilly.org

Compliance Risks

Privacy and Data Security Risks
Data breaches occur when unauthorized access occurs to sensitive, personal, or confidential data. They can lead to financial losses, reputational damage, and legal action. Patient data is sensitive and must be protected from unauthorized access. Data automation can increase the risk of data breaches if security measures aren't in place.

Billing and Coding Errors
Billing and coding compliance is vital to quality and practice success and errors can have serious consequences. Upcoding is a common coding and billing compliance risk that can lead to False Claims Act allegations, financial settlements, and corporate integrity agreements.

Anti-kickback violations
The Anti-Kickback Statute (AKS) is a federal criminal law prohibiting exchanging anything of value to induce or reward referrals for businesses that federal health care programs can reimburse. The AKS applies to both the payer and recipient of kickbacks. Violating anti-kickback laws can severely affect healthcare providers, including exclusion from federal healthcare programs, including Medicare and Medicaid.

Fraudulent Activities
Fraudulent claims can include knowingly presenting false or fraudulent claims for payment or approval. This can also include making or using false records or statements concerning the submission of such claims.

Creating a Compliance Plan: The 7 Elements

1. Implementing Written Policies and Procedures
2. Designating a Compliance Officer and/or Committee
3. Effective Training & Education
4. Open Lines of Communication
5. Enforcement and Disciplinary Guidelines
6. Risk Assessment, Internal Auditing & Monitoring
7. Prompt Response to Offenses and Corrective actions

1. IMPLEMENTING WRITTEN POLICIES AND PROCEDURES

Code of Conduct

Your organization's Code of Conduct articulates your commitment to complying with all Federal and State laws and regulations. It defines all ethical standards necessary to fulfill the organization's mission. It governs the conduct of its officers, employees, contractors, and others who work with or on behalf of the organization.

Compliance Policies and Procedures

Compliance policies and procedures should encompass at least two areas: implementing and operating your compliance program, including the seven elements and processes to reduce risks caused by noncompliance with Federal and State laws. You should assess how your operations may present risk areas specific to your program and design policies and procedures that address the risks mentioned in the Compliance Risks slide.

Policy Maintenance

All relevant individuals should be able to easily access your organization's code, policies, and procedures. It is not unusual for providers to maintain their code, policies, and procedures on an internal intranet site or use other electronic communication tools to ensure everyone can access the same documents. The OIG recommends that programs should set up a regular schedule for reviewing and revising, as necessary, all policies and procedures. Additionally, policies and procedures should be reviewed at least annually to ensure that such policies and procedures reflect any modifications to applicable statutes, regulations, and Federal health care program requirements.

2. DESIGNATING A COMPLIANCE OFFICER AND/OR COMMITTEE

Designation of a compliance officer and/or compliance committee accountable and responsible for the activities and status of the compliance program, including issues identified, investigated, and resolved by the compliance program. It is important to note that the Senior management and applicable body (such as a board) must be engaged and reasonably oversee the compliance program.

The Compliance Officer (CO) should report directly to the CEO with direct and independent access to the board. The CO's responsibility is to oversee and monitor the implementation and operation of the compliance program, be able to revise the compliance program as needed and coordinate with other relevant internal entities like those who conduct internal auditing, quality assurance teams, and IT, for example, to develop work plans for reviewing, monitoring and auditing compliance risks.

2. DESIGNATING A COMPLIANCE OFFICER AND/OR COMMITTEE

To be effective, a compliance program should have a board and senior leadership that understand its value and are committed to its success. One of these senior leaders should be the Compliance Officer (CO).

Compliance Officer and Committee Should:
- Meet no less than quarterly
- Analyze the legal and regulatory requirements
- Assess, Develop, and Regularly Review Policies and Procedures
- Monitor and Recommend Internal Systems and Controls
- Assess Education and Training Needs
- Develop an Environment that Promoted Compliance Reporting
- Conduct Annual Risk Assessments

3. EFFECTIVE TRAINING AND EDUCATION

Effective Training and Education

This covers the elements of the compliance plan and preventing, detecting, and reporting FWA. Tailor this training and education to the employees and their responsibilities and job functions. Training should occur annually and incorporate material addressing any concerns identified in audits and investigations. All board members, officers, employees, contractors, and medical staff (if applicable) should receive training on your compliance program and potential compliance risks.

Education should not be limited to annual formal training requirements. The compliance officer should seek and develop opportunities to provide education on compliance topics and risks throughout the year. Some Education topics to consider are Risk identification and mediation, Billing, Coding, and Documentation Standards.

- Development of an Annual Training Plan
  - Training Plans should include Education and Training on your Compliance Program
  - Training Materials should be widely available
- Specific Topic Examples
  - Risk Identification and Mediation
  - Billing, Coding, Documentation Standards

4. OPEN LINES OF COMMUNICATIONS

Open Lines of Communication

An open line of communication between the compliance officer and personnel (including contractors and agents) is critical to successfully implementing a compliance program and reducing any potential for fraud, waste, and abuse. Effective lines of communication should be accessible to all, ensure confidentiality, and provide methods for anonymous and good-faith compliance issues.

Written confidentiality and nonretaliation policies should be developed and distributed to all employees. All disclosures of compliance concerns, including potential violations of your program's policies or Federal or State requirements, should be recorded in a log maintained by the compliance officer or someone designated to do so by the compliance officer. All disclosures should be logged promptly, regardless of how they are made.

- All Staff should be able to have at least one reporting path independent of the business and operational functions that permit them to report concerns anonymously: a hotline, a website, an email address, or a mailbox.

- Disclosures of all compliance concerns need to be logged promptly.

5. ENFORCEMENT & DISCIPLINARY GUIDELINES

Enforcement & Disciplinary Guidelines

For a compliance program to be effective, your organization should establish appropriate consequences for instances of noncompliance. Consequences may be educational or remedial and non-punitive; they may be punitive sanctions or involve both. The consequences of noncompliance should be consistently applied and enforced to deter noncompliant conduct. All levels of employees should be subject to the same consequences for the commission of similar offenses.

This information should be made available to all levels of the organization.

6. RISK ASSESSMENT INTERNAL AUDITING & MONITORING

Risk Assessment, Internal Auditing & Monitoring

Risk assessment, auditing, and monitoring each play a role in identifying and quantifying your organization's compliance risk. A compliance risk assessment is a process that looks at the risk to the organization stemming from violations of law, regulations, or other legal requirements. Periodic compliance risk assessments should be a component of your organization's compliance program and should be conducted at least annually.

- The Compliance Committee should include a schedule of audits based on risks identified by the annual risk assessment in its compliance work plan. The Compliance Committee should also ensure the compliance officer can perform or oversee additional audits based on risks identified throughout the year.

- Depending on the size of your staff and the resources available, you may have dedicated compliance auditors reporting to the compliance officer to conduct these audits. The compliance work plan should also contain routine monitoring of ongoing risks, plus the capacity to monitor the effectiveness of controls and risk remediation.

- Conducting routine monitoring and auditing of operations is important to evaluate the overall effectiveness of the compliance program.

7) PROMPT RESPONSE TO OFFENSES AND CORRECTIVE ACTIONS

Prompt response to offenses and corrective actions

Responding to offenses and developing corrective action initiatives are important parts of an effective compliance program. These steps help maintain the program's integrity and ensure that violations are remediated quickly and without reoccurrence.

Compliance programs should include processes and resources to investigate compliance concerns thoroughly, take the steps necessary for remediation (including reporting to any Government program agencies or law enforcement where appropriate) , and analyze the root cause(s) of any identified impropriety to prevent a recurrence.

7) PROMPT RESPONSE TO OFFENSES AND CORRECTIVE ACTIONS

Tips for Responding to Offenses Found

Designate a reviewer: When a compliance incident occurs, a compliance officer or other designated employee should review the allegation to determine whether it's a violation and whether corrective action is needed. Smaller programs may designate someone, such as the compliance contact, to carry out these steps.

Investigate Thoroughly: Most internal investigations will require interviews and a review of relevant documents. Based on the potential scope and severity of the suspected violation and the necessary investigative tasks, you should consider whether they need to engage external counsel, auditors, or other experts to aid the investigation.

Report Violations: If credible evidence of misconduct from any source is discovered and, after a reasonable inquiry, the compliance officer or counsel has reason to believe that the misconduct has occurred, the provider should promptly notify CBH's Program and Integrity Department and appropriate Government authority of the misconduct.

Corrective Actions: Once you have gathered sufficient credible information to determine the nature of the misconduct, you should take prompt corrective action, including refunding overpayments, enforcing disciplinary policies and procedures, and making any policy or procedure changes necessary to prevent a recurrence.

ADDITIONAL RESOURCES

US Department of Health and Human Services Office of Inspector General (OIG) General: Compliance Program Guidance

CBH Provider Manual

Questions or Comments

Andrew Robertson
andrew.robertson@phila.gov