ATRÓMITOS
CONSULTING DONE FEARLESSLY

Conducting a Compliance Readiness Assessment

Contracting as a Medicaid provider brings with it a significant increase in regulatory contract compliance requirements and scrutiny. This requires that a contracting organization have a coherent and robust compliance program able to:

1. **Identify** areas of risk;
2. **Prevent** non-compliance through the use of internal controls including the education and training of workforce members;
3. **Detect and Investigate** non-compliance;
4. **Report** (as indicated) **and Correct** non-compliance; and
5. **Monitor and improve** performance over time.

Many community-based organizations and nonprofits providing Permanent Supportive Housing (PSH) and other services operate with limited resources and low overhead. Smaller organizations often have not had to invest in or stand up the kind of formalized compliance operations that are required for Medicaid contracting.

How to Use this Toolkit

The purpose of this toolkit is to provide practical guidance for how an organization can evaluate the effectiveness and adequacy of its compliance operations as it adapts to becoming a Medicaid provider.

This process involves four steps:

1. Identify the objectives and requirements of operations (what are the programmatic and regulatory requirements of operations? What are the areas of risk for the organization?)
2. Ensure that there are written policies and procedures touching on each area of compliance. These policies and procedures describe how the organization implements these programmatic and regulatory requirements in practice, so they must be "comprehensive" and inclusive of the full scope of risk of the organization.
3. Evaluate the *effectiveness* of written policies and procedures **and** of the mechanisms to monitor and evaluate the performance of the compliance program.
4. Once gaps in the content of the organization's policies and procedure or the application of the compliance program are identified, identify the steps to close those gaps.

The first section of this toolkit (Step One) provides a simplified framework which organizations can use to identify and organize the various categories of contractual and regulatory compliance which must be met. It walks through common Medicaid provider requirements and provides a template which organizations can use to identify their own areas of risk to be managed.

Once an organization understands the scope of compliance requirements (and risk exposure), the next step is to validate that the organization has a formal system for ensuring that the operational compliance with those contractual, professional, and regulatory requirements. This is first demonstrated by written policies and procedures. This includes not only the policies and procedures governing specific programmatic requirements (i.e., an organizational policy directing how Protected Health Information is used within an organization) but *also* the policies and procedures governing compliance operations themselves.

In other words, the mechanisms by which the organization ensures that substantive policies and procedures are adhered to and that violations are detected and responded to effectively. That includes things like (1) identification of a compliance officer; (2) description of ways that team members can report incidents; (3) how incidents are investigated, responded to, and corrected; and (4) how team members are trained on policies and procedures, on areas of risk and expectations of performance.

Finally, in any readiness evaluation there are two key questions. The first is general how effectively an organization can identify risk, prevent or deter violations, detect and address incidents, and continuously improve. The "Seven Essential Elements of an Effective Compliance Program" discussed in the second section of this tool kit (Step Two) outline how to evaluate compliance operations *as a whole* and the adequacy of the organizational infrastructure. The second question is if an organization's policies and procedures sufficient to cover the scope of all operations *specific to* individual regulatory and contract requirements and areas of risk. This means that, for example, a healthcare provider (or FCS provider who has executed a Business Associate Agreement with a covered entity) has a written policy and procedure for every element of HIPAA requirements as it foreseeably intersects with that organization's operations.

This analysis is specific to the content of an organizations policies and procedures based on its regulatory risk exposure and contract requirements. The devil is always in the details. For this reason, the Toolkit concludes with a high-level walk through of the regulatory requirements in one area regulatory compliance (HIPAA) as an example of how an organization can break down compliance requirements to ensure that policies and procedures are sufficient both "on paper" and in practice.

Step One: Identifying (and Understanding) Standard Compliance Requirements

The first step in evaluating the adequacy of an organization's compliance operations is to define the objectives of the compliance program. Broadly speaking compliance operations exist in order to ensure that an organization adheres to all regulatory and contract requirements, professional standards and ethical obligations and to identify and manage organizational risk. One of the biggest challenges when evaluating an organization's "readiness" to contract as a Medicaid provider is identifying and understanding the "universe" of contract and regulatory requirements and industry standards that apply.

The breadth of regulatory and contract compliance requirements in healthcare contracting (generally) and Medicaid contracting (specifically) can feel overwhelming, however, these requirements can *generally* be thought of as falling into the six broad categories:

1. Record Keeping and Documentation,
2. Fraud, Waste, and Abuse Prevention, Detection, and Reporting,
3. Privacy and Security,
4. Quality Assurance and Reporting,
5. Professional and Ethical Standards, and
6. Federal and State Regulatory Compliance.

Table 1 below describes each of these categories and provides an example of where such a requirement can be found in the FCS Participating Provider Agreement (2023). Please note that Table 1 is intended only to illustrate how compliance requirements are knitted throughout the Agreement. As such, it provides only one or two examples in each category **and is not a complete or comprehensive catalog of contract or regulatory compliance requirements.**

TABLE 1. ILLUSTRATIVE EXAMPLES OF CATEGORIES OF COMPLIANCE REQUIREMENTS

Category	Description	Example(s)
Record Keeping and Documentation	Providers are required to maintain accurate and updated documentation to support the delivery of and billing for their services. Statutory regulations and contract terms require a minimum period of document retention. Records are subject to audit by the Third-Party Administrator, the State, and CMS representatives.	Section 6.18 (Right to Review Records/Availability of Records); Section 7.1 (Records)
Fraud and Abuse Prevention, Detection, and Reporting (i.e., Program Integrity)	Providers are directly subject to state and federal regulations including the False Claims Act and CMS's compliance program. Providers also have a positive duty to implement controls to prevent, detect, report and correct instances of suspected fraud, waste and abuse of program resources. Finally, by contract Provider agrees to be subject to an cooperate with Amerigroup's anti-fraud compliance program and related policies and procedures.	Section 3.12 (Reporting Fraud and Abuse), Section 3.13 (Conformance with Law)
Privacy and Security (including HIPAA)	As a contracted Medicaid Provider an FCS provider is subject to HIPAA as a business associate of Amerigroup. This includes a duty to protect the confidentiality, integrity, and accessibility of protected health information (PHI). This requires the development of written policies, procedures and other controls to ensure adherence to HIPAA, including (but not limited to) appropriate use, required accounting and documentation of HIPAA operations and PHI disposition.	Section 5.1 (Business Associate Agreement); Section 3.10(b) (Proprietary Information, Confidentiality); Section 7.1 (Records).
Quality Assurance and Reporting	Providers are responsible for exchanging data in order to coordinate and manage care; to adhere to regulatory, professional and programmatic quality standards in the delivery and reporting of care (this includes timeliness and appropriateness of services). Provider must have an internal quality assurance mechanism to monitor and report on the quality of services delivered. Provider shall be subject to and cooperate with Amerigroup's Quality Assurance program and its policies and procedures. Material violation of Amerigroup's quality assurance standard is a basis for immediate termination of the agreement by Amerigroup. Provider will submit a monthly report on all covered members and quarterly progress reports to demonstrate performance outcomes and quality improvement activities.	Section 3.7 (Compliance with Credentialing, Utilization Management, Quality Assurance, Grievance, Coordination of Benefits); Section 6.19 (Provider to Monitor Quality); Appendix A (Provider Qualifications, 2a Adherence to Quality Standards Supportive Housing); Appendix A (Provider Qualifications, 3 (Administration); Appendix A (Reports Monitory, Quality Standards and Deliverables.
Professional Standards	Providers are responsible for adhering to all professional standards including licensures, scope of work, and relevant standards of practice.	Section 3.2 (Licensure and Accreditation); Section 3.7 (Compliance with Credentialing, Utilization Management, Quality Assurance, Grievance, Coordination of Benefits)
Compliance with State and Federal Laws	This is always the biggest, broadest and generally most vaguely defined category in a Provider Agreement. Important areas of federal and state laws and regulations include (but are not limited to): • Non-Discrimination, anti-Harassment requirements • Compliance with the Americans with Disabilities Act • Annual Financial Auditing and Reporting requirements (which may vary dependent upon revenue volume and source of funds) • Prohibition against anti-competitive practices • Prohibition against retaliation of whistleblowers • Performance of services within the United States • Availability of interpreter services for Medicaid members	Article VI (Compliance with Regulatory Requirements); Section 6.1 (Compliance with Regulatory Requirements); Section 6.4 (Non-Discrimination); Section 6.11 (Compliance with Federal Regulations)

APPLICATION

The first step, therefore, in evaluating an organization's compliance "readiness" is to identify what that organization has to comply with. The following template can be used by an organization's compliance officer to "brainstorm" the scope of compliance requirements and risk exposure by each of these categories. The Template (Table 2) is divided into two domains, the first (Existing Requirements) references those requirements that an organization had to comply with prior to becoming a Medicaid Provider.

The second domain (FCS Contract Requirements) is for the identification of those new requirements imposed by the new FCS contract. Begin by filling out those requirements that the organization must meet today (Existing Requirements). Then review the FCS Contract and add new or expanded requirements in the right-hand column. Creating this side-by-side will enable the organization to clearly see the extent of the changes required to become an FCS-compliant provider.

this space is intentionally blank

TABLE 2. COMPLIANCE REQUIREMENTS TEMPLATE

Category	Existing Requirements	FCS Contract Requirements
Record Keeping and Documentation		
Program Integrity		
Privacy and Security (including HIPAA)		
Quality Assurance and Reporting		
Professional Standards		
State and Federal Laws		

Step Two: The Seven Essential Elements of a Compliance Program

Once an organization has determined the scope of regulatory (and contract) risk exposure, the next step is to evaluate the adequacy of the organization's mechanisms to promote compliance and risk management.

There is no "one size fits all" when it comes to what constitutes a robust or adequate compliance program across the healthcare industry. Recognizing this, the Office of the Inspector General for the Department of Health and Human Services has identified what it describes as the "Seven Essential Elements of a Compliance Program." While the compliance controls and the systems to monitor, detect, and correct compliance violations vary based on operations, size, and risk profiles, every compliance program must have each of these components, which are illustrated in Table 3, below.

Table 3. Description of the Seven Essential Elements of a Compliance Program

Element	Description
Written Policies and Procedures	Written policies and procedures exist that comprehensively outline the compliance program, workforce responsibilities, and the organization's commitment to compliance with relevant regulations and requirements. These policies clearly outline standard expectations, are regularly reviewed, updated and communicated to employees and reflect the full scope of operations.
Designation of a Compliance Officer and Compliance Committee	There is a designated officer within the organization with the authority and responsibility for the development and administration of the compliance program. Reporting pathways exist to enable adequate oversite by the governing board.
Effective Training and Education	Training education programs are implemented to educate workforce members of the compliance program, policies and procedures, and compliance responsibilities.
Reporting	There must be multiple effective lines of communication across the organization to enable reporting of compliance incidence to the compliance officer and compliance committee, including the ability to submit anonymous reports and a guarantee and protection against the threat of retaliation.
Auditing and Monitoring	An organization has and deploys systems and mechanisms to (1) assess the effectiveness of the compliance program and identify areas for improvement and (2) identify, deter and correct violations. This includes regular and periodic audits; risk assessments, and use of data analytics and surveillance or monitoring systems.
Corrective Action	There is a formal process governing the timely investigation and response to compliance issues, including corrective actions to address violation or areas of identified risk.
Enforcement and Disciplinary Standards	An organization enforces compliance with its policies and procedures through disciplinary standards or sanctions in the event of non-compliance.

APPLICATION

With that background in the "essential elements" of a compliance program, the next step is to apply them to the organization. This can be divided into (1) the "content" and contextual adequacy of the organization's policies and procedures as it relates to each of the six domains identified in Step One and (2) the effectiveness of the infrastructure and mechanisms in place to ensure that those policies and procedures are adhered to across the organization (i.e., element 2-7 of the "Seven Essential Elements). For the purposes of this Toolkit, this will focus on how to determine the content adequacy of policies and procedures.

1. For each of the six domains, consider the following questions:
2. Does the organization have a policy or procedure addressing each required element of that domain?
3. Is there are formal process for the development, modification and update of policies and procedures to ensure that they are reflective of all areas of risk and changing requirements?
4. Do policies provide adequate detail on the procedures necessary to follow in order to comply? (i.e., Policies are not just broad statements of 'commitment to compliance' but include clear and complete procedures as to the application of that policy in usual operations).
5. Do written policies and procedures identify who is accountable for
    a. Performing specific compliance functions? (eg: conducting OIG required exclusion searches of staff and vendors? Maintaining HIPAA disclosure accounting logs?)
    b. Monitoring and evaluating adherence to procedures?
    c. Receiving and responding to compliance issues?
6. Do written policies and procedures adequately address all (relevant) operations?

Once the organization can evaluate the content adequacy of each area of risk (i.e., the six compliance domains), it can evaluate how well the organization's compliance infrastructure and compliance program *operates as a whole*.

Step Three: Zooming in on Specific Compliance Requirements—Sample HIPAA Compliance Assessment Template

Recognizing that one of the hardest parts in a compliance readiness evaluation is understanding the scope of the requirements that need to be implemented and monitored, the final section of this toolkit provides a high-level walkthrough of the components that must be addressed by an organization's Privacy and Security Policies in order to comply with Health Insurance Portability and Accountability Act (HIPAA). HIPAA was selected as an example because it is an area of regulatory compliance which many PSH providers have likely not had to deal with in previous operations.

It is, therefore, likely that many organizations will not have existing HIPAA policies and procedures. This template, Table 4, therefore, provides a detailed description of the components that need to be addressed in those policies. In addition to being a tool to evaluate compliance with HIPAA requirements, this table can also be used as a simplified "Table of Contents" to guide both the development of new policies as well as to guide the detailed evaluation of existing ones.

It should be noted that the proposed template provides a *simplified* snapshot, identifying at a high level the minimum standards associated with HIPAA Privacy and Security Regulations that need to be reflected in an organization's Policies and Procedures. The table identifies the general requirements in the first column, then details component elements of each category in the following column.

Users should use the third column (titled "Policy") to cite the organization's Policy that addresses each of the component parts of a general requirement. Multiple policies may cover each requirement, each should be referenced. The final column (Action Needed) is where the user identifies the gaps that exist (i.e., where there isn't a policy or procedure addressing a component of a requirement) and details the steps needed to address the gap.

this space is intentionally blank

TABLE 4. SAMPLE HIPAA COMPLIANCE ASSESSMENT TEMPLATE

General Requirement	Component Parts	Policy	Action Needed
Defines HIPAA Privacy, Security and Breach Notification requirements.	• HIPAA regulatory requirements and responsibilities and defined and program for (and organizational commitment to) compliance is outlined. • Process by which policies reviewed on an annual and periodic basis		
Appoint of Privacy and Security Officers and description of mechanisms to administer Privacy and Security program and conduct oversight	• Privacy Officer identified and responsibilities outlined. • Security Officer identified and responsibilities outlined. • There is a meaningful process and reporting pathway by which the board can exercise oversight. • Process by which policies reviewed on an annual and periodic basis		
Appropriate access to, use and disclosure of PHI	• Defines permitted and non-permitted use of PHI and outlines the procedures and controls related to approved use. • Defines permitted and non-permitted disclosure of PHI and outlines the procedures and controls for each. • Defines required disclosures of PHI and the procedures associated therewith. • Provides examples of permitted and non-permitted use and disclosure of PHI specific to the organization's routine operations.		
Minimum Necessary Use and Disclosure of PHI	• Defines the standard of "Minimum Necessary Use or Disclosure." • Access to PHI is stratified based on job functions. • Provides criteria and examples to guide application of "Minimum Necessary" standard that are relevant to organization's operations.		
Patient Right of Access and other Rights	• Includes the policies and procedures to ensure compliance with Patient's right to access, copy and request corrections to PHI and the associated notice and timeliness standards. • Organization publishes Notice of Privacy Practices for reference by patients.		
Accounting and Record Retention	• Disclosure of PHI that is not subject to (1) a written authorization or (2) an exemption (i.e., Treatment, Payment, Operations), must be documented. • Accounting of Disclosures and documentation related to the administration of the HIPAA compliance program must be retained for a minimum of 6 years.		

General Requirement	Component Parts	Policy	Action Needed
PHI Disposition and Destruction	• Details the administrative, technological, and physical controls to ensure the confidentiality, integrity, and accessibility of PHI, including controls specific to the security of electronic PHI. Controls exist for PHI that is retained/stored, exchanged, and associated with its destruction.		
Minimum Security Standards	• The program details the administrative, technological and physical controls required of individual users to protect PHI AND across the organization and system. Examples include: password protection standards, use of firewalls, encryption, locked doors and storage. • Specific protections are applied to ePHI. • Organization conducts annual and periodic risk assessments to confirm or correct the adequacy of security controls.		
Monitoring and Auditing	• There exist mechanisms to evaluation effectiveness of the HIPAA privacy and Security program and detect noncompliance including pathways to report issues. • These mechanisms and systems are tailored to the operations and risks of the organization.		
Training	• There is a program to train workforce members on HIPAA policies and procedures, enforcement, and reporting pathways. Training includes awareness of risks to electronic data and systems.		
Investigations and Incident Responses	• There are formalized procedures and resources allocated to investigated incidents of potential noncompliance. • Where there is a breach of PHI, this includes completion and documentation of a breach risk assessment to determine responsibilities to report to business associate and up to DHHS. Policies and procedures include evaluation and implementation of corrective action or to otherwise mitigate impact.		
Sanctions	• There are formal disciplinary sanctions associated with violation of HIPAA controls and policies and procedures. Sanctions are tailored to the factors associated with a violation and are sufficient to serve as a deterrent.		

ENDNOTES

[1] DHHS, Office of the Inspector General, "The Seven Fundamental Elements of an Effective Compliance Program," Available at: https://oig.hhs.gov/documents/provider-compliance-training/945/Compliance101tips508.pdf.