

Conducting a Behavioral Health Risk Assessment

Tim Timmons, CCEP, CHP, CHPC, CHSS
Privacy and Security Officer
Greater Oregon Behavioral Health

Todd Jacobson, LCSW, CHC
Compliance Officer
Greater Oregon Behavioral Health



What will we cover today?

- ▶ The risk assessment process
 - ▶ Definitions
 - ▶ Scope
 - ▶ Risk categories
 - ▶ Conducting the assessment

- ▶ Identifying behavioral health compliance risks
 - ▶ Fee-for-service vs. capitation
 - ▶ Governing body
 - ▶ HIPAA and Part 2
 - ▶ Other risk areas



Definitions

- ▶ Risk analysis - A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.
- ▶ Under the HIPAA Security Rule, a "risk analysis" requires entities to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."



Definitions

- ▶ Risk assessment - Risk assessment is the determination of quantitative or qualitative estimate of risk related to a recognized threat. Quantitative risk assessment requires calculations of two components of risk: the magnitude of the potential loss, and the probability that the loss will occur.
- ▶ In the Breach Notification Rule a risk assessment is what an entity must conduct in order to determine whether there is a low probability that protected health information has been compromised, which informs whether the breach notification requirements will come into play. 45 CFR 164.402



Scope of the Risk Assessment

- ▶ Fraud, waste or abuse
 - ▶ Federal Sentencing Guidelines
- ▶ Civil or criminal risk exposures
 - ▶ False Claims Act
- ▶ Legal or contractual risks
 - ▶ Contracts with the state
 - ▶ Managed care/provider/subcontractor contracts
- ▶ Any potential liability to the organization



Some Risk Categories

- ▶ Competitors
- ▶ Governance
- ▶ Reputational
- ▶ Leadership
- ▶ Financial
- ▶ Client satisfaction
- ▶ Delegated responsibilities



The Risk Assessment Process

- ▶ Identify key internal stakeholders
- ▶ Identify all the significant compliance risks to which the organization is exposed (See handout for risk categories)
- ▶ Each of those risks should be discussed to inform all the stakeholders about the nature of the risks
- ▶ Rate each risk according to the following criteria:
 - ▶ Level of threat - what is the likelihood of an incident occurring?
 - ▶ Impact - the effect a particular incident would have (this could include direct costs, legal liability and loss of reputation or goodwill)



The Risk Assessment Process

- ▶ After all of the risks in the inventory have been scored using the criteria above, the next step is to prioritize them
- ▶ The next step in the process is to select the risks that the organization chooses to target for remediation/mitigation during a specified period of time, usually one year. This step in the process recognizes that no organization has unlimited resources to address every possible risk that has been identified, but that the most serious risks need to be identified and addressed first.



The Risk Assessment Process

- ▶ Consider the following before developing a plan for mitigating the priority risks.
 - ▶ Avoid the risk by discontinuing the risky practice
 - ▶ Control or mitigate the risk
 - ▶ Accept the risk
 - ▶ Transfer the risk through insurance, subcontracts
- ▶ Consider developing your own internal compliance risk mitigation plan, especially if the risk is internal and there is leadership reluctance



Managed Care vs Fee-for-Service

- ▶ Fee-for-service is characteristically managed by the state
 - ▶ No fixed payments - Providers bill for services delivered and are paid on predetermined rates for each service
- ▶ Managed care is subcontracted to managed care entities (MCEs)
 - ▶ A fixed per capita payment made periodically to a practitioner or provider by a managed care entity in return for covered services provided to enrolled individuals
- ▶ Both are governed by the Mental Health Parity and Addictions Equity Act of 2008



Risk Areas - Capitation and Fee-for-Service

- ▶ Inadequate provider network- Client is unable to access care or unable to obtain quality of care
- ▶ Prohibited relationships - Transparency of ownership or controlling interest and its impact on decision making
- ▶ Absence of an ethics and compliance program that contains the elements contained in the Federal Sentencing Guidelines



Risk Areas - Capitation and Fee-for-Service.

- ▶ Service Delivery - Under fee-for-service, lack of validation that service were delivered. Under capitation, not meeting state or MCE quality expectations
- ▶ Insufficient or lack of documented compliance training
 - ▶ Especially emphasizing the False Claims Act, protection for whistleblowers and identified priority risk exposures
- ▶ Failure to track or identify invalid claims



Compliance Risks Under Managed Care

- ▶ Quality of Care Standard
 - ▶ Mikes v. Strauss - leading quality of care decision.
 - ▶ Implied certification = a claim for payment is legally false under the FCA "only where a party certifies compliance with a statute or regulation as a condition to government payment."
 - ▶ Quality of care theory (worthless service) = Cannot merely challenge the level of care, but must allege that any care provided was equivalent to no care at all.



Compliance Risks Under Managed Care

- ▶ Provider misrepresentation of performance via attestation or report submissions.
 - ▶ Collecting correct information, yet provider attestation or reporting is dubious.
- ▶ MCE failure to specify delegated requirements
 - ▶ MCE does not collect correct information from participating providers or subcontractors, thus failing to identify worthless services which creates a risk to clients.



Compliance Risks Under Managed Care

- ▶ State mandated performance requirements
 - ▶ Quality standards - HEDIS & CAHPS
 - ▶ Inadequate performance results in sanctions. Prolonged sanctions result in loss of contract.



Compliance Risks Under Managed Care

- ▶ Failure to have an adequate provider network - resulting in underutilization, which is one of the most significant False Claims Act risks in managed care
- ▶ Abuse is a greater risk than fraud
 - ▶ Payment for services that are medically unnecessary or fail to meet professionally recognized standards of care
 - ▶ Rather than restricting access, billing for everything to increase your allocation during next rate setting process (Oregon biennially)



Compliance Risks under Fee-For-Service

- ▶ Overutilization
 - ▶ Recommending or providing services which are not medically necessary
 - ▶ Billing for services that were not provided
 - ▶ Upcoding



Compliance Risks under Fee-For-Service

- ▶ Accuracy/completeness of claims or encounters
 - ▶ Coding errors
 - ▶ Insufficient documentation to support the claim (more critical on FFS)



Other Behavioral Health Risk Exposures

- ▶ HIPAA and 42 CFR Part 2
 - ▶ More confidentiality restrictions for federally assisted drug and alcohol treatment programs
 - ▶ Challenges posed by a mandate to integrate care
 - ▶ Access to an integrated health record containing both A&D and mental health services
 - ▶ Risks to the provider if it isn't defined as a hybrid organization - Part 2 restrictions prevail for all PHI
 - ▶ Staff ignorance of both HIPAA and Part 2 restrictions on the use and disclosure of PHI



Other Behavioral Health Risk Exposures

- ▶ Provision of services to individuals with limited English proficiency (LEP)
 - ▶ Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d
 - ▶ Executive Order 13166 - Each federal agency that extends federal financial assistance is required to issue guidance explaining the obligations of their recipients to ensure meaningful access by LEP persons to their federally assisted programs and activities
 - ▶ DOJ policy guidance - See handout



Other Behavioral Health Risk Exposures

- ▶ Recipients are required to take reasonable steps to ensure meaningful access to their programs and activities by LEP persons. While designed to be a flexible and fact-dependent standard, the starting point is an individualized assessment that balances the following four factors:
 - (1) The number or proportion of LEP persons eligible to be served or likely to be encountered by the program or grantee;
 - (2) The frequency with which LEP individuals come in contact with the program;



Other Behavioral Health Risk Exposures

- ▶ Recipients are required to take reasonable steps to ensure meaningful access to their programs and activities by LEP persons. While designed to be a flexible and fact-dependent standard, the starting point is an individualized assessment that balances the following four factors:
 - (3) the nature and importance of the program, activity, or service provided by the program to people's lives; and
 - (4) the resources available to the grantee/ recipient and costs



Governance Risk Exposures

- ▶ Conflicts of interest (perceived and actual), particularly in rural areas
- ▶ Violation of the board's fiduciary duty of care - determining whether the directors:
 - ▶ Acted in good faith
 - ▶ With the level of care that an ordinarily prudent person would in like circumstances
 - ▶ In a manner that they reasonably believe is in the best interest of the organization



Governance Risk Exposures

- ▶ Not fulfilling its fiduciary duty of care by making inquiries to ensure: (1) a corporate information and reporting system exists, and (2) the reporting system is adequate to assure the Board that appropriate information relating to compliance with applicable laws will come to its attention timely and as a matter of course (See handout from the OIG/AHLA/AHIA/HCCA)
- ▶ Conflicts of interest (perceived and actual), particularly in rural areas



Other Risk Exposures

- ▶ Risks associated with services such as therapeutic foster care
- ▶ Safety risks related to in-home services
- ▶ Credentialing risks
- ▶ Corporate culture - staff turnover
- ▶ Insufficient or ineffective compliance training
- ▶ Rapid growth
- ▶ Subcontractor non-compliance



QUESTIONS?

Tim Timmons
tim.timmons@gobhi.net
503-931-9867

Todd Jacobson
todd.jacobson@gobhi.net
541-298-2101

