COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY AND PROCEDURES MANUAL				
Chapter **Program Quality**	**Section** **Compliance**	**Chapter** **05**	**Section** **04**	**Subject** **04**
Subject **Risk Assessment**	**Authorization**		**Approved: 11/29/05** **Replaces: None**	

Reviewed/No Updates: May 2022

I. PURPOSE: To establish a risk assessment process for compliance and to manage risk and reduce the severity of a loss if one were to occur.

II. APPLICATION: All programs of Community Mental Health Authority.

III. DEFINITIONS:

A. Risk:

1. The net impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur.

2. Exposure to the chance of injury or loss. The risk can be external (i.e., natural disaster) or internal (i.e., back injury while performing job duties).

B. Risk Assessment: Typically, a broad-based audit that may be used to identify opportunities for improvement either before development of the compliance program or work plan or periodically, thereafter. A systematic and effective method of identifying risks and determining the most cost-effective means to minimize or remove them.

C. Risk Factors: Aspect of personal behavior or lifestyle, environmental exposure, or variable or condition that increases the likelihood of an adverse outcome.

D. Threat: The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

E. Vulnerability: A flaw or weakness in procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a risk.

IV. POLICY: Risk assessments will be performed, as needed, by an individual or group designated by the Chief Executive Officer.

V. PROCEDURE:

A. NorthCare Network's Compliance Risk Assessment, developed by the regional Corporate Compliance Committee, may be utilized as a risk assessment tool.

B. The tool includes pre-determined Risk Categories, Specific Risks, and Primary Area(s) Affected. Areas to be determined are:

1. Likelihood of risk occurrence

2. Severity of risk
3. Financial cost
4. Non-financial cost (human factor)
5. Priority rank

C. Identify the scope of the risk assessment. The scope of a risk assessment may vary from narrow to broad. For example, a narrow scope assessment of "billing" may focus on a specific area such as coding. A broad scope assessment of billing may encompass activity logs, progress notes, plan of service, coding, and Medicaid bills.

D. Gather data. Once the scope of the risk assessment is identified, relevant data should be gathered. Relevant data may be gathered by reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques.

E. Identify and document potential threats and vulnerabilities. The identification of threats and vulnerabilities could be separated into two distinct steps but are so closely related in the risk assessment process that they should be identified at the same time. Independent identification may result in large lists of threats and vulnerabilities that, when analyzed (in subsequent steps to identify risk), do not provide valuable information.

1. Identify and document threats. To start, CMHA may compile a categorized list of threats (such as natural, human, and environmental). CMHA may identify different threats unique to the circumstances of its environment. CMHA should focus its list of threats to those that are reasonably anticipated. After the complete list is compiled, it should be reduced to only those reasonably anticipated threats. This can be done by focusing on specific characteristics of the entity in relation to each of the threat categories. For example, CMHA's geographic location will determine the natural threats that may create a risk. A hurricane is a threat, but in CMHA's area, it probably would not be considered a reasonably anticipated threat. Human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. Potential human sources that could trigger or exploit vulnerabilities are employees (the most common source), ex-employees, business rivals, terrorists, criminals, general public, vendors, customers, and visitors. Anyone that has the access, knowledge, and/or motivation to cause an adverse impact can act as a threat.
2. Identify and document vulnerabilities. While identifying potential threats, CMHA must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk. The process of identifying vulnerabilities is similar to the process used for identifying threats. CMHA should create a list of vulnerabilities, both technical and non-technical. There are numerous sources of information to review when identifying and documenting both technical and non-technical vulnerabilities. Sources of information to identify non-technical vulnerabilities may include previous risk assessment documentation, audit reports, or security review reports. Sources of information

to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories. The internet is a valuable resource for sharing technical vulnerability lists and advisories. It contains sites that provide information on specific technical vulnerabilities and the mechanisms for sign-up and distribution of technical vulnerability advisories.

F. Assess current safeguards. The goal of this step is to analyze current safeguards implemented to minimize or eliminate risk. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective safeguards have been implemented. The output of this step should be documentation whether safeguards are already in place and if they are configured and used properly.

G. Determine the likelihood of threat occurrence. Likelihood of occurrence is the probability that a threat will trigger or exploit a specific vulnerability. Each potential threat and vulnerability combination will be rated by the likelihood (or probability) that the combination will occur. Likelihood will be rated by Rare, Unlikely, Likely, Very Likely, Almost Certain.

H. Determine the potential impact of threat occurrence. If a threat triggers or exploits a specific vulnerability, there are many potential outcomes. The impact of potential outcomes will be measured in order to prioritize risk mitigation activities. The qualitative method of measurement will be used (i.e., work groups, interviews, direct observation, document analysis, etc.). The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale of Rare, Unlikely, Likely, Very Likely, Almost Certain. This method will allow the measurement of all potential impacts, whether tangible or intangible.

I. Determine the severity of risk. The severity of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The severity of risk determination is based on the assigned likelihood of threat occurrence and resulting impact of threat occurrence. The severity of risk determination utilized will be Insignificant, Minimal, Moderate, Severe, Very Severe but Recoverable, and Catastrophic.

J. Identify the actions required to manage the risk. Once risk is identified and assigned a severity of risk level, actions will then be identified to manage the risk.

VI. REFERENCES AND LEGAL AUTHORITY: DHHS HIPAA Security Series Volume 2 Paper 6; National Institute of Standards and Technology Special Publication 800-30; NorthCare Network’s Compliance Policies; CARF Behavioral Health Standards

VII. EXHIBITS: None