County of San Bernardino
Department of Behavioral Health

Risk Assessment Policy

Effective Date 2/1/07
Approval Date 2/1/07

Allan Rawland, Director

Policy

It is the policy of Department of Behavioral Health (DBH) to assess risks to information assets and manage those risks effectively by reducing threats of impairment to the confidentiality, integrity and availability of such assets. A standard risk assessment methodology and management process will be used for all systems used to create, store, process or transmit internal, confidential, restricted or critical information.

Purpose

DBH requires system owners and responsible units to conduct risk assessments on all information technology systems, devices and related equipment, and update such risk assessments as needed in order to manage risks effectively. Units may request assistance with conducting the required assessments for their area/system(s) by contacting the department's Privacy and Security Officer or Information Technology. Information systems/application risk assessments must be conducted periodically and as part of the procurement process for all systems. Policies and procedures developed for compliance with this policy must be forwarded to the department Privacy and Security Officer for review.

Risk Assessment

1. The risk assessment process is used to identify and assess risks associated with information assets and define cost-effective solutions to managing those risks.

2. An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of information should be conducted for all systems and applications that contain confidential or restricted information. The scope of the risk assessment will include the administrative, physical and technical controls as required by law and the DBH privacy and security policies.

3. Risk assessment is the first and one of the most important steps in the security management process. An assessment of assets, risks to those assets, and the development of countermeasures to those risks must be conducted. In addition, implementations of other DBH security policies are dependent on the thoroughness and quality of risk assessment.

Frequency for Conduction Risk Assessments

Risk assessments shall be conducted/reviewed annually. In addition, an assessment shall be performed under each of the following special circumstances:

- Purchase, acquisition or procurement
- Part of the system development/modification/upgrade process
- When changes are to be made to the infrastructure (e.g. remodel, additions, installations, etc.)

Standard Risk Assessment Process

The department's Privacy and Security Officer will develop a standard risk assessment process to be used, which includes:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and other management staff as necessary.

2. Identification of the information assets that are at risk, with particular emphasis on the applications of information technology that are critical to patient care and business operations.

3. Identification of the threats to which the information assets could be exposed.

4. Assessment of the vulnerabilities, i.e., the points where information assets lack sufficient protection from identified threats.

5. Determination of the impact of loss, based upon quantitative or qualitative assessment of a realized threat for each vulnerability and an estimation of the likelihood of such occurrence.

   Note: As part of the determination, actual or planned countermeasures, which may be installed must be ignored and considered to be not present. This is because it is the intrinsic importance (value) of the data itself which needs to be assessed, If existing countermeasures were taken into account this would artificially deflate the essential value of the data. The fact that the security breaches may be countered or the consequences prevented or minimized is not relevant to the assessment at this point.

6. Identification and estimation of the cost of protective measures that would eliminate or reduce the vulnerabilities to an acceptable level of risk.

7. Selection of cost-effective security management measures to be implemented.

8. Preparation of a final report to be submitted to the Privacy and Security

Officer by Information Technology and to be kept on file the department, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of remaining risk to be accepted.

Risk Assessment Steps

The computer security risk management guidance published by the National Institute for Standards and Technology (NIST) in its Special Publication (SP) 800-30 titled "Risk Management Guide for Information Technology Systems" should be used as a guide in conducting information security risk assessments compliant with the above requirements. This publication describes the following nine risk assessment steps that should be used in conducting the required risk assessments. Scoring has been added to each required area as necessary to provide consistency.

Step	Action	Description
1.	**System Characterization**	Document the system/application, purpose, owner or responsible person(s), department, location, contact information, function, connectivity, number and type of users, physical environment description and system/application criticality as defined below: **Determine system/application criticality multiplier as follows** — **Level** / **Score** CRITICAL - Data is vital to patient care — High 2.0 ESSENTIAL - Data is crucial for operations, not critical to patient care — Medium 1.5 IMPORTANT - Data is needed to conduct business, but not essential — Low 1.0
2.	**Threat Identification**	Identify the potential threat-sources and compile a list of potential threat-sources and associated vulnerabilities that are applicable to the system being evaluated. (NOTE: for compliance with the HIPAA Security rule, the required administrative, physical and technical safeguards are used to define the threat/vulnerability list.) Each of the listed threats is then assigned a score based on the threat it poses to one or more of the required confidentiality, integrity and availability requirements.
	Vulnerability Identification	Identify flaws or weaknesses that could be exercised to result in a security breach or violation of the system's security policy. (Note: for compliance with the HIPAA Security Rule, the required administrative, physician and technical safeguards are used to define the threat/vulnerability list.) Each of the listed threats/vulnerabilities is then assigned a score based on the threat it poses to one or more of the required confidentiality, integrity and availability requirements.

3.		**Threat/Vulnerability could result in** — **Level** — **Score** Loss of Confidentiality, Integrity and Availability (CIA) — High — 10 Los of Confidentiality and Integrity (CI) — Medium — 5 Loss of Confidentiality and Availability (CA) — Medium — 5 Loss of Availability and Integrity (AI) — Medium — 5 Loss of Confidentiality (C) — Low — 1 Loss of Integrity (I) — Low — 1 Loss of Availability (A) — Low — 1
4.	**Impact Analysis**	Determine the adverse impact from a successful threat exercise of vulnerability. The adverse impact shall be categorized accordingly: loss of integrity, loss of availability, and loss of confidentiality. **Impact** — **Level** — **Score** Exercise of threat/vulnerability could: Severely impact operations and resources — High — 10 Moderately impact operations and resources — Medium — 5 Minimally impact operations and resources — Low — 1
5.	**Likelihood Determination**	To derive an overall rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. Determine the probability that this threat will occur if no safeguards are in place to prevent it. **Likelihood** — **Level** — **Score** Very likely to occur — High — 2.0 Likely to occur — Medium — 1.0 Not likely to occur — Low — 0.5
6.	**Control Analysis**	Analyze the controls that have been implemented, or are planned for implementation, to minimize or eliminate the likelihood (or probability) of a threat exercising a system vulnerability. Note: If safeguards are in place then such safeguards serve as a countermeasure to the associated threat thereby reducing the risk that a threat/vulnerability will occur to an acceptable level.
7.	**Risk Score Determination**	Calculate level of risk to system/application to determine its overall risk. A system or applications risk score is calculated by performing the following computation for each threat identified and averaging those risk scores for an overall Risk Score.

		Risk Score = Data Criticality x Threat/Vulnerability x Impact x Likelihood Risk Scores, using the above scoring, will range from 1 – 200. High and medium risk systems must be corrected and a new risk assessment must be completed to bring the system/application into the acceptable risk score range (LOW). Risk ratings are based on the risk score as shown below: **System/Application Risk Priority** — **Risk Score Range** **High** - Countermeasures are required immediately to reduce risk — 50-200 **Medium** - Create plan to reduce risk to an acceptable level — 0-49 **Low** - System risk is within the "acceptable Range — 1-9
8.	**Remediation/ Corrective Action**	Controls/Safeguards to mitigate (reduce) or eliminate the identified risks, as appropriate, must be identified and corrective action taken for systems/applications, with scores above the LOW or 1-9.9 range.
9.	**Results Documentation**	Once the risk assessment has been completed, the results will be documented in an official report and made available to the Behavioral Health Privacy and Security Officer or their designee and to the appropriate unit manager/system owner and Assistant Director. Risk assessments must be maintained for a minimum of six years from the time created or last in effect.

Risk Management

System owners and department managers/supervisors are responsible for risk management. These decisions must be based on the results of the required risk assessment process above. The department manager/application owner is responsible for prioritizing, implementing, and maintaining the appropriate risk-reducing measures identified from the risk assessment process.

Implementation of security measures sufficient to reduce risks and vulnerabilities to information systems and resources to a reasonable and appropriate level are required in order to:

- Ensure the confidentiality, integrity, and availability of all sensitive information created, received, maintained, or transmitted
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
- Ensure compliance with this policy by department staff, contract providers, vendors and business associates

Residual Risk

Even after implementing all security controls, no covered entity will be 100 percent risk free or 100 percent secure. Many times after a security control is implemented, there is some amount of risk remaining, which is called the residual risk. In addition, a residual risk exists when a decision is made to accept a risk due to the cost of the control being high or the likelihood or impact of the threat being low. Management must determine the amount of residual risk to accept. The risk assessments should provide management with enough information to make decisions about residual risks.

There are four basic ways of addressing residual risk:

1. Transferring - If management decides that the total or residual risk is too high, it may purchase insurance to offset any costs should the risk be realized. For a cost which is less than the control, they are transferring the risk to the insurance company.

2. Rejecting - If management ignores the risk they are choosing to reject it in theory, but practically, are accepting it because the risk and the liability does not just go away (see number 4 below – Accepting risk).

3. Reducing - If management implements controls, they are reducing or mitigating the risk.

4. Accepting – If management decides to live with the identified risk, they are accepting the impact of it should it be realized. Normally the "residual" risk is accepted AFTER mitigating or correcting the initial risk and lowering it to an acceptable level.

Note: DBH must utilize numbers 3 and 4 "Reducing" and "Accepting" risk in order to maintain compliance with regulations and best practices for information security.

Workforce Sanctions (Disciplinary Action)

Behavioral Health must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the department. The "workforce" is defined as employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DBH, is under the direct control of DBH, whether or not they are paid by DBH.

Standard sanction levels include types of sanctions and instances in which they can be applied for privacy and security violations. Sanctions are based on the relative severity of the violation and related privacy and security policies. Sanctions (disciplinary action) must be documented and maintained for the six (6) year minimum period required.

Information Systems Activity Review (Periodic Review of Internal Security Controls)

Each information system owner/responsible unit must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports to identify discrepancies between policies and practices. A "system" normally includes hardware, software, information, data, applications, communications, and people.

- Monitoring should be performed by use of the audit capabilities of the access control software system and through the internal creation and use of programs specific to this purpose as approved by Information Technology and the department's Privacy & Security Officer.

- Upon notification of any abnormal activity, the information system/application owner/responsible department must review the incident and take appropriate action and follow-up.

Periodic Physical Security Risk Assessment

Each department/area will:

- Establish and document procedures for performing periodic self-assessments of security controls.
- Perform initial and periodic risk assessments on systems processing or storing confidential or restricted information.
- Perform initial and periodic physical and technical security risk assessments according to DBH's Physical Security Policy.
- Maintain risk assessments in secured files. Correct identified problems.
- Forward risk assessments to the DBH Privacy and Security Officer upon request

Frequency of System and Physical Security Assessments

- Assessments should be conducted <u>annually</u> for existing systems/areas. New assessments will be required under the following circumstances:
  - System procurement
  - Systems development or post installation
  - Major changes to the building or system infrastructure
  - Upon notification of a vulnerability or violation or breach of privacy or security

- The system owner/unit manager is responsible for implementing changes in policies, procedures and system modifications necessary to mitigate security risks to an acceptable level based upon assessment findings.

- Assessments (and reports after remediation of the findings) must be retained for six (6) years from the date of creation or the date when the document last was in effect, which ever was later.

Violations of the Use of Behavioral Health Systems

Staffs that violate the use of DBH systems as described above or in other County policies will be subject to disciplinary action that can include termination of employment.

References

HIPAA SECURITY RULE REQUIREMENTS:

- **Security Management Process (Required) [45 C.F.R § 164.308(a)(1)(i)]**
  Implement policies and procedures to prevent, detect, contain, and correct security violations.

- **Risk Analysis (Required) [45 C.F.R § 164.308(a)(1)(ii)(A)]**
  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.

- **Risk Management (Required) [45 C.F.R. § 164.308(a)(1)(ii)(B)]**
  Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with section 164.306(a).

- **Information System Activity Review (Required) [45 C.F.R. § 164.308(a)(1)(ii)(D)]**
  Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

- **Evaluation Standard § 164.308(a)(8)**

- **Section 164.316** – outlines the requirements for developing security policies and procedures. Policies and procedures must be updated when there is a change in the law; an environmental or operational change that affects the security of the PHI; and/or a change in practices.