DAVIS BEHAVIORAL HEALTH
Community · Commitment · Change

Policies & Procedures

RISK MANAGEMENT POLICY

Section: HIPAA

Pages: 5

Subject: Risk Management

Effective Date: 08/2017

Revision Date: 05/03/2023

Purpose:

This policy establishes the scope, objectives, and procedures of Davis Behavioral Health's (DBH) information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

Policy:

1. It is the policy of DBH to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its protected health information (PHI) and to develop strategies and policies to efficiently and effectively mitigate the risks identified in the assessment procedure as an integral part of the organization's information security process.
2. Risk analysis and risk management are recognized as important components of DBH's corporate compliance program and information technology (IT) security process.
   A. Risk assessments are done throughout IT system life cycles:
      i. Before the purchase or integration of new technologies, changes are made to physical safeguards.
      ii. While integrating technology and making physical security changes; and
      iii. While sustaining and monitoring appropriate security controls.

   B. DBH performs periodic technical and non-technical assessments of the security rule requirements as well as in response to operational changes affecting the security of PHI. Results are made available to the Executive Leadership Team (ELT) for review and assessment of risk.
3. DBH implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   A. Ensure the confidentiality, integrity, and availability of all PHI the organization creates, receives, maintains, and/or transmits,

B. Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI,
C. Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required, and
D. Ensure compliance by workforce.

4. All DBH employees are expected to fully cooperate with all persons charged with doing risk management work. All risk management efforts, including decisions made on what controls to put in place as well as those not to put into place, are discussed and documented at ELT meetings on a quarterly basis or as needed.

Scope

The scope of the information security risk management process covers the administrative, physical, and technical processes that enable and govern PHI that is received, created, maintained, or transmitted.

Key Definitions:

Protected Health Information (PHI): Any individually identifiable health information protected by HIPAA and 42 CFR Part 2 that is transmitted or stored.

Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of PHI and other confidential or proprietary information.

Risk Assessment: the process:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact.
- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk Management: Within this policy, it refers to two major process components: risk assessment and risk mitigation.

Risk Mitigation: Referred to as *Risk Management* in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within DBH given its mission and available resources.

Threat: the potential for a particular threat to successfully create vulnerability.

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

Procedures: The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of DBH's ELT, corporate compliance officer and DBH's contracted IT provider.

Risk Assessment: The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

Step 1. System Characterization

The first step in assessing risk is to define the scope of the effort. To do this, identify where PHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).

Step 2. Threat Identification

In this step, potential threats (the potential for threat-sources to successfully identify a particular vulnerability) are identified and documented. Consider all potential threat-sources to help generate a list of potential threats.

Step 3. Vulnerability Identification

The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern DBH's computer usage to insufficient safeguards to protect computer equipment to copy room PHI, email, text, fax etc.

Step 4. Likelihood Determination

The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.

Step 5. Impact Analysis

The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to DBH's mission; sensitivity and importance; costs associated; loss of confidentiality and integrity.

Step 6. Risk Determination

This step is intended to establish a risk level. By multiplying the ratings from the impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed. The risk rating also presents actions that ELT should take for each risk level

Step 7. Control Recommendations

The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

Step 8. Results Documentation

Results of the risk assessment are documented in an official report or briefing and provided to ELT to make decisions on policy, procedure, budget, and system operational and management changes

Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk- reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of PHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

Step 1. Prioritize Actions –

Using results from Step 6 of the Risk Assessment, sort the threat and vulnerability information according to their risk-levels. This establishes a prioritized list of actions needing to be taken.

Step 2. Conduct Cost-Benefit Analysis –

Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its cost of application. Areas that are not cost-effective are also identified during this step.

Step 3. Select Control(s) –

Taking into account the information and results from previous steps, DBH's mission, and other important criteria, the ELT will prioritize areas for reducing risks to the information systems and to the confidentiality, integrity, and availability of PHI.

Step 4. Assign Responsibility –

ELT will identify the individual(s) or team with the skills necessary to implement each of the specific areas outlined in the previous step and assign their responsibilities. ELT will also identify the equipment, training and other resources needed for their successful implementation. Resources may include time, money, equipment, etc.

Risk Management Schedule: The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of DBH's information security program:

Scheduled Basis – an overall risk assessment of DBH's information system infrastructure will be conducted every two years.

As Needed – the corporate compliance officer or ELT may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect DBH's information systems.

References: 45 CFR 164.308(a)(1)(i) and (ii)(A-B).