PURPOSE
To establish requirements and steps the DEPARTMENT will use to identify and mitigate risks to electronic protected health information (ePHI).

POLICY

RISK ANALYSIS
1. DEPARTMENT will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).
2. DEPARTMENT DIRECTOR will ensure a risk analysis is:
   a. Performed every 3 years,
   b. Reviewed quarterly, and
   c. Updated as needed.
3. DEPARTMENT DIRECTOR will ensure the risk analysis includes:
   a. A defined scope that identifies all systems that create, transmit, or maintain ePHI,
   b. Details of identified threats and vulnerabilities,
   c. An impact and likelihood analysis,
   d. An assessment of current security measures, and
   e. Risk rating.
4. DEPARTMENT DIRECTOR will maintain risk analysis documentation for six years.
5. Workforce members will cooperate with those performing the risk analysis.

RISK MITIGATION
1. DEPARTMENT DIRECTOR will:
   a. Establish a departmental Risk Management Team (RMT) that includes workforce members, senior management, and key decision makers.
2. The RMT will:
   a. Review threats and vulnerabilities quarterly and as needed.
   b. Address risks according to the risk rating.
   c. Select actions and implement measures that mitigate risk to an acceptable level.
   d. Document the actions taken to mitigate risks.
   e. Document actions “in progress” that will mitigate risks.
   f. Document and retain approval decisions.

PROCEDURE

RISK ANALYSIS
The intent of a risk analysis is to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).

The analysis will follow these steps:

- **STEP 1** – Define the scope by identifying where ePHI is created, transmitted, or maintained. This can be accomplished with a variety of techniques, such as interviews, sensitive data scans, or creating ePHI flow maps.
- **STEP 2** – Identify and document potential threats and vulnerabilities. Consider threats that, if exploited, would create a risk of unauthorized access or disclosure.
- **STEP 3** – Determine the likelihood that a threat will occur.
- **STEP 4** – Determine the potential impact of threat occurrence. Use a qualitative or quantitative method (or a combination of both) to rate the impact each occurrence could have.
- **STEP 5** – Assess current security measures. Identify current security measures (technical or non-technical) that could mitigate the likelihood of a threat occurring.
- **STEP 6** – Determine the level of risk considering impact, likelihood, and current security measures.
- **STEP 7** – Document the results. Ensure the results are documented and in a usable form. One the department can use to easily demonstrate the analysis and its outcome.
RISK MITIGATION
The intent of a risk mitigation is to choose and implement measures that mitigate risk to an acceptable level. Steps in this process include:

- **STEP 1** – Rank the identified threats and vulnerability pairs by risk level. Then, identify the highest risk threats to address.
- **STEP 2** – Identify potential controls that can mitigate the threat.
- **STEP 3** - Determine which controls are most feasible. Feasibility can include many factors, such as cost, complexity, and effectiveness.
- **STEP 3** – Select the best control to mitigate risk.
- **STEP 4** – Identify and assign an individual the responsibility to implement the selected control.
- **STEP 5** – Gain and document the DEPARTMENT DIRECTOR’s approval.
- **STEP 6** – Implement the control.
- **STEP 8** – Determine and document how and how often the control will be reviewed to ensure its effectiveness.
DEFINITIONS

1. **Workforce member** - Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

2. **Vulnerability** - A flaw or weakness in procedures, design, implementation, or controls that could be triggered or exploited and result in a security breach or a violation of security policy.

3. **Threat** – The potential for a person or thing to exercise (trigger or exploit) a specific vulnerability.

4. **Risk** – A function of 1) the likelihood of a given threat triggering or exploiting a vulnerability, and 2) the resulting impact on the organization.

5. **Electronic Protected Health Information (ePHI)** - Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.