HIPAA SECURITY: RISK ANALYSIS

POLICY:

Lifesong Hospice and Palliative Care conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the hospice's electronic protected health information.

DEFINITIONS:

Vulnerability:
Technical or non-technical flaws or weaknesses in security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of security policies.

Threat:
The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. Examples of different types of threats include, but are not limited to:

- ***Natural -*** *floods, earthquakes, tornadoes, and landslide*
- ***Human -*** *intentional actions (e.g., network and computer based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional actions (e.g., inadvertent data entry or deletion and inaccurate data entry)*
- ***Environmental*** *- power failures, pollution, chemicals, and liquid leakage*

Risk:
A function of:

1. *The likelihood of a given threat triggering or exploiting a particular vulnerability, and*
2. *The resulting impact on the organization.*

PROCEDURE:

1. Lifesong Hospice and Palliative Care has a comprehensive and accurate understanding of the technical and non-technical components of its security environment related to electronic protected health information (PHI).

2. The hospice's risk analysis considers all the electronic PHI it creates, receives, maintains or transmits.

Created:	Reviewed:	Revised:	Effective:
05/2018	11/2018		4/2019

3. At a minimum, the risk analysis process includes, but is not limited to:
    a. Identifying and documenting where electronic PHI is stored, received, maintained or transmitted;
    b. Identifying and documenting specific, reasonably anticipated threats to electronic PHI;
    c. Identifying and documenting vulnerabilities, which if triggered or exploited by a threat, might create a risk of inappropriate access to or disclosure of electronic PHI;
    d. Assessing and documenting the security measures Lifesong Hospice and Palliative Care uses to safeguard electronic PHI and their effectiveness;
    e. Determining the likelihood of threat occurrence with consideration of the impact of potential risks;
    f. Assessment of the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability; and
    g. Assignment and documentation of risk levels for all threat and vulnerability combinations identified during the risk analysis that includes a list of corrective actions to be performed to mitigate each risk level.

4. A comprehensive risk analysis report summarizes the findings of the risk analysis.

5. The risk analysis report is retained for six (6) years from the date completed or last updated, whichever is later.

6. Risk analyses are conducted on an ongoing basis and specifically when:
    a. New technologies and/or business operations are planned;
    b. Lifesong Hospice and Palliative Care has experienced a security incident;
    c. There has been a change in ownership; and/or
    d. There is a turnover in key staff or management.