

Lifespan Corporation Policy

Subject:

Policy on Evaluating the Effectiveness of Security Policies and Procedures

File Under:

HIPAA Security

Issuing Department(s):

Information Services

Latest Revision Date:

July 29, 2015

Last Review Date:

July 2015

Original Policy Date:

October 14, 2014

Policy Number: HSP-85

Page 1 of 2

Approved By:


CISO


CIO

Policy on Evaluating the Effectiveness of Security Policies and Procedures

Introduction

Lifespan has adopted this Policy on Determining the Effectiveness of Security Policies and Procedures in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

Lifespan hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs periodic Evaluations of the Effectiveness of Security Policies and Procedures for Lifespan. All personnel of Lifespan must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- ❑ Lifespan hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.
- ❑ Lifespan must comply with HIPAA and the HIPAA implementing regulations pertaining to the periodic evaluation of the effectiveness of security policies and procedures, in accordance with the requirements at § 164.308(a)(8).
- ❑ Security policies and procedures, including emergency and contingency plans and procedures, must be evaluated periodically to determine their potential effectiveness in genuine emergencies.

Policy Statement

- ❑ It is the Policy of Lifespan to periodically evaluate security policies and procedures, including emergency and contingency plans and procedures, in order to improve their effectiveness.

Procedures

- ❑ It shall be the responsibility of the Office of the CISO to periodically conduct such technical and nontechnical evaluations.
- ❑ The Office of the CISO shall work in coordination with legal counsel, information services, senior management, and any other persons, departments or parties necessary in order to conduct such evaluations.
- ❑ Such technical and nontechnical evaluations shall be conducted at least annually as well as when any of the following events occur:
 - There is a change to any state or federal regulation that may affect the Security Policies
 - There is a new state or federal regulation that may affect the Security Policies
 - There has been a significant breach of security or other security incident within Lifespan
 - Any other time the Office of the CISO feels there is a need to evaluate the Security Policies
- ❑ The results of such technical and nontechnical evaluations shall be internally published and shall be available to senior management and to all parties with responsibility for emergency preparedness.
- ❑ The purpose of such evaluations is to improve the effectiveness of Lifespan's security policies and procedures, including emergency and contingency plans and procedures, so that they best protect the business, the assets, the personnel, and the individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) that Lifespan possess or uses.
- ❑ The Office of the CISO shall fully document the periodic technical and nontechnical evaluations to determine the effectiveness of Lifespan's security policies and procedures, including emergency and contingency plans and procedures, in accordance with the Documentation Policy and the requirements of HIPAA.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with Lifespan's Sanction Policy.