Helios Network System Security Plan

Prepared by the Information Technology Department,
Helios Health Insurance

Executive Summary

Helios Health Insurance is required to identify all components of the network that contains, processes, and transmits data and information to help prepare and implement a plan for the security and privacy of the data and information. The objective of network system security planning is to improve the protection of all network resources. The Helios network has some level of sensitivity and requires protection as part of best management practices. The protection of the network must be documented in a network system security plan (NSSP). The security plan is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a network. It reflects direct collaboration from management responsible for the various network components and processes.

The purpose of this NSSP is to provide an overview of the security of the Helios Health Insurance network and to describe the controls and critical elements in place. This NSSP follows guidance contained in NIST Special Publication (SP) 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems, February 2006.*

Note: The NSSP is a living document that will be updated periodically to incorporate new and/or modified security controls. The plan will be revised as the changes occur to the technical environment.

1. **System Name and Identifier**

System Name	HNSSP

2. **System Categorization**

FIPS 199 Guide for Developing Security Plans
Potential Impact

Security Objective	Low Impact	Moderate Impact	High Impact
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security Objective	Low Impact	Moderate Impact	High Impact
Integrity: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability: Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

3. **System Operational Status**

Operational	Under Development	Major Modification
Server Cluster, Printing Management, End Users, System Administrators, Remote Users	Security Cluster	None

4. **Information System Type**

Major Application	General Support System
Server Cluster, Security Cluster, Printing Management	End Users, System Administrators, Remote Users

5. **System Environment**

Helios Health Insurance is a standalone enterprise network that contains organized suites of hardware and software configurations. These configurations consist of managed workstations and servers protected from the internet by various network security devices. The list below illustrates the breakdown of the environment to include both hardware/software and administrative processes.

- **Network-Wide**
  - Workstations, including laptops, have a baseline image configuration that keeps the hard drives unencrypted for faster hard drive performance.
  - Open access to WIFI.
  - End user computers have full access to the internet and are not patched or updated regularly.
- **Remote Users**
  - Mobile users are local administrators on the laptops.
- **System Administrators**
  - Telnet to switches by administrators.
  - System admin network behind a firewall.
- **Server Cluster**
  - FTP to file server uses default admin account.
  - Web server uses SSL.
  - Mail server does not have quota requirements set on the end user mailbox.
- **Security Cluster**
  - Security cluster has an application-scanning server and a digital certificate server to better secure the server cluster.
- **Printing Management**
  - Printers, scanners, and copiers are not patched regularly.

6. **Laws, Regulations, and Policies Affecting the System**

The following laws or regulations establish specific requirements for the confidentiality, integrity, or availability of the data in the system. The following laws or regulations apply to the Helios Health Insurance network system, which handles protected health information (PHI): HIPAA and HITECH.

7. **Minimum Security Controls**

Appropriate minimum security controls were implemented, and a baseline (low, moderate, or high impact) was documented using NIST SP 800-53 as guidance. This baseline document can be found in Appendix A.

Network System Security Plan Approval Date: March 2, 2016