OHIP DOS
System Security Plan Overview
v 1.6
September 21, 2015

Table of Contents

1 PURPOSE

New York State Office of Health Insurance Programs (OHIP) is responsible for providing guidance and oversight for Medicaid related information systems, programs and business processes at the Department of Health (DOH). This responsibility includes defining business, information, and technical guidance that will create a common security framework for IT system implementations responsible for protecting DOH Medicaid data. OHIP extends this guidance to entities with whom DOH provided Medicaid data is shared. The guidance and security framework is based on the set of NIST 800-53 recommended security controls for government information systems at the moderate level with enhancements that are necessary to comply with NYS Policies and Standards (aka Moderate Plus).

As part of DOH's Data Exchange Application and Agreement (DEAA) data sharing agreements, business partners who desire access to DOH provided Medicaid data are required to compete System Security Plans (SSPs) that document which controls have been implemented and how for all systems that are used to house and process the DOH provided Medicaid Data.

The SSP consists of two parts:

1. System Security Plan Overview (this document), along with supporting attachments, as described in Section 2 System Identification and subsequent sections, to provide context for the SSP Control Workbooks. Respondents should use this document as a template for providing the information requested.
2. SSP Control Workbooks, organized by NIST 800-53 control family that provide information on specific security controls implemented by the organization on relevant systems used to house and process DOH provided Medicaid Data.

2 SYSTEM IDENTIFICATION

When completing the SSPs, organizations should provide the system identifiers, which include the official name and/or title of system, including acronym for the primary system as well as dependent systems covered by this plan. Also provide the contact information for the organization responsible for the systems within scope of the SSPs. The tables below identify the primary system that is responsible for storage and processing of the Medicaid Data as well as dependent systems. The *primary system* is the main system that is maintaining and storing DOH Medicaid data. *Dependent systems* are other systems connect to or in some way supporting access to the data from the primary system. Examples of dependent systems would include Identity and Authentication systems, Audit systems etc. Dependent systems are other systems used by the primary system to support the primary systems functioning. Organizations should use the table templates below to document their systems. Completion of the PPS templates will include references back to the named systems here as needed.

TABLE 1 – SYSTEM IDENTIFICATION

Primary System Name	
System Acronym *(if used)*	
Purpose of System	
Operational Status*	
Organization	
Owning Organization	
Contact for Questions (Name)	
Contact email address	
Contact Phone Number	
Alternate Contact Name and Phone Number	
Description of Business Process and system usage	

Dependent System Name	
System Acronym *(if used)*	
Purpose of System	
Operational Status*	
Organization	
Owning Organization	
Contact for Questions (Name)	
Contact email address	
Contact Phone Number	
Alternate Contact Name and Phone Number	
Description of Business Process and system usage	

*The General Support System (GSS) or Major Application (MA) is New, Operational, or Undergoing Major Modification

3 DESCRIPTION OF THE BUSINESS PROCESS

Provide a description of the business processes supported by each system, including any business system diagrams. This information will provide context for understanding the environment and reason behind the implementation of controls. For this section and its subsections, do not duplicate information that is included in the SSP workbooks. When appropriate, provide a reference to the control that provides the desired information.

- Describe how information flows through/is processed by the system, beginning with system input through system output. Further describe how the data/information is handled by the system (is the data read, stored, purged, etc.)
- Describe the dependencies, i.e. other business processes and resources that support each business function. This includes the required inputs (business functions/processes that feed this function), processing functions (calculations, etc.), organizational/personnel roles and responsibilities, and expected outputs/products (that may "feed" other business functions / processes;
- Indicate the organizations (internal & external) that will comprise the user community. Include type of data and processing that will be provided by users, if any.
- Indicate, the physical location of the business processes and technology that will support the process.

Description of the Business Process

4 SYSTEM OVERVIEW

Provide a brief overview of the purpose and capabilities of the primary system. For this section and its subsections, do not duplicate information that is included in the SSP workbooks. When appropriate, provide a reference to the control that provides the desired information.

Primary System Overview:

4.1 SYSTEM OPERATING ENVIRONMENT

Provide a brief description of the system operating environment:

- Is the system owned or leased?
- Is the system operated by the State or by a support service contractor? If the system is operated by the state run consolidated data center, provide the name, location and point of contact for the consolidated data center.
- If the system is maintained or "run" by a contractor, describe (comprehensively) how the system is managed.
- Document the hours of operation: e.g. 24x7, M-F 7:30 am – 5:00 pm.
- Document the approximate total number of user accounts and unique user types (i.e. researchers, programmers, administrative support, caseworkers, public-facing employees, etc.).
- Identify the critical processing periods (e.g., eligibility processing.).

System Operating Environment Description:

4.1.1 Security Concerns

Describe any environmental or technical factors (vulnerabilities or pre-disposing conditions) that raise special security concerns for the system, for example:

- The use of BYOD, tablets, smartphones, wireless technology, etc.
- The system is connected to the Internet;
- The physical location of the information system;
    - It is located in a harsh or overseas environment;

- It is located at a facility outside of State control.

- Software is implemented rapidly

Primary System Overview:

4.2 ARCHITECTURE AND TOPOLOGY

4.2.1 Network Diagrams

Attach a diagram or diagrams which illustrate the network connectivity including the system components' connection, and the security devices, which 1) protect the system; and, 2) monitor system access and system activity. For systems that have more than one server of the same type, only include one in the diagram; however state the accurate count of the servers in the supporting text description.

4.2.2 System Logical Diagrams

Also include logical diagrams as necessary to illustrate data flows among system components and system boundaries, to clarify understanding of the system function and integration.

4.2.3 Architecture Description

Describe the architecture of the network and information system illustrated in the diagrams provided above. Be sure to number system components in the diagrams to correlate with the information presented in the diagrams. Include text that will explain system components, connectivity and function including the following:

- Describe the network topology.
- Describe the hardware, software, and system interfaces (internal and external) to include interconnectivity.
- Describe the network connection rules for communicating with external information systems.
- Describe the functional areas within the architecture (presentation, application and data zones, if applicable) and how this addresses security.
- Describe the boundary of the information system for security accreditation.
- Describe the information flow or processes within the system to access to the data/information.

4.3 IDENTITY ASSURANCE LEVEL

Respondents must complete the Identity Assurance Worksheets for the systems covered by this plan. The worksheets are included in the Appendices of the New York State ITS Identity Assurance Policy NYS-P10-006 and further described in the New York State ITS Identity Assurance Standard NYS-S13-00, linked below:

http://www.its.ny.gov/document/identity-assurance-policy

http://www.its.ny.gov/document/identity-assurance-standard

5 SSP CONTROL WORKBOOKS OVERVIEW

The SSP Control workbooks are intended to provide the details of the organizational system security plan, describing what controls have been implemented along with details on how they have been implemented sufficient to ensure DOH that the controls are in place and operational. The SSPs can be used in two ways by organizations receiving provided Medicaid data:

- If organizations have existing system security plans, then the SSPs can be completed by referencing their existing plans where existing plans document the relevant control and how it is implemented.
- If organizations do not have existing system security plans then the SSPs can serve to become the organizations security plan.
- When providing SSPs to DOH the completed SSP and any supporting documentation that is needed to support the particular control documentation should also be provided.

When completing the SSPs, organizations should describe the controls that exist on systems containing DOH provided Medicaid data. When completing an individual control description the organization should address the control as it exists on all relevant systems. Therefore, the description for a given control may be different for the various systems and applications where the control has been implemented.

The attached document provides guidance on how to complete the System Security Plan (SSP) Control Workbooks, including two completed control examples. These workbooks provide details on how the required security controls are implemented by the organization for the covered system.

OHIP SSP Procedure
with Eight Examples