PROGRAM MANAGEMENT BUSINESS AREA
SECURITY AND PRIVACY (SP) CHECKLIST

STATE:	DATE OF REVIEW:	REVIEWER:

SECURITY AND PRIVACY (SP) CHECKLIST

SECURITY AND PRIVACY CHECKLIST BACKGROUND

Background for this checklist:

1. Within the Health Insurance Portability and Accountability Act (HIPAA) there are two separate Rules governing Privacy and Security.
    a. The Privacy Rule deals with the Rights of individuals to safeguard the privacy of their health care information. Privacy Rule compliance is under the jurisdiction of the Office for Civil Rights.
    b. The Security Rule deals with the requirements of facilities, systems, and processes to safeguard information for which it is liable.
2. There is an overlap between parts of the Privacy Rule and the Security Rule. The overlap occurs when the MMIS is the vehicle or enabler of the process that enforces the Privacy requirements. For this reason, Privacy and Security requirements are combined into one checklist.
3. MMIS certification focuses on system functionality. To enforce compliance with the full range of Privacy and Security requirements, the Medicaid agency uses a range of reports, alerts, audits, and surveys. These are beyond the scope of MMIS certification. This checklist focuses on those functions within an MMIS that demonstrate the agency's ability to meet the system-related requirements of Privacy.

Sources for the criteria in this checklist are as follows:

IBP – Industry Best Practice. Items are selected from RFPs for MMISs developed by states and approved by CMS.

CFR – Code of Federal Regulations, available from http://www.access.gpo.gov/uscode/title42/title42.html. Includes HIPAA Security and Privacy rules.

BUSINESS OBJECTIVES

Reference #	Business Objectives	Comments
SP1	Control access to system and data.	

PROGRAM MANAGEMENT BUSINESS AREA
SECURITY AND PRIVACY (SP) CHECKLIST

BUSINESS OBJECTIVES		
Reference #	**Business Objectives**	**Comments**
SP2	Protect the confidentiality and integrity of electronic Protected Health Information (ePHI).	
SP3	Monitor system activity and act on security incidents.	
SP4	Support individual rights specified in the HIPAA Privacy regulations.	
SPSS1	*Add State-specific business objective for the Security and Privacy Checklist here.*	

SP1 – CONTROL ACCESS TO SYSTEM AND DATA					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP1.1	Verifies identity of all users, denies access to invalid users. For example: ▪ Requires unique sign-on (ID and password) ▪ Requires authentication of the receiving entity prior to a system-initiated session, such as transmitting responses to eligibility inquiries	CFR			
SP1.2	Enforces password policies for length, character requirements, and updates.	CFR			
SP1.3	Supports a user security profile that controls user access rights to data categories and system functions.	CFR			

PROGRAM MANAGEMENT BUSINESS AREA
SECURITY AND PRIVACY (SP) CHECKLIST

SP1 – CONTROL ACCESS TO SYSTEM AND DATA					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP1.4	Permits supervisors or other designated officials to set and modify user security access profile.	CFR			
SP1.5	Includes procedures for accessing necessary electronic Protected Health Information (ePHI) in the event of an emergency; continue protection of ePHI during emergency operations.	CFR			
SP1.6	Supports workforce security awareness through such methods as security reminders (at log on or screen access), training reminders, online training capabilities, and/or training tracking.	CFR			
SP1.7	Contains a data classification schema with data items flagged to link them to a classification category and has an access privilege scheme for each user that limits the user's access to one or more data classification categories.	IBP			
SP1.8	Alerts appropriate staff authorities of potential violations of privacy safeguards, such as inappropriate access to confidential information.	CFR			
SP1.9	Contains a data definition for the Designated Record Set (DRS) that allows it to be included in responses to inquires and report requests.	CFR			
SP1.10	Supports data integrity through system controls for software program changes and promotion to production.	IBP			

PROGRAM MANAGEMENT BUSINESS AREA
SECURITY AND PRIVACY (SP) CHECKLIST

SP1 – CONTROL ACCESS TO SYSTEM AND DATA					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP1SS.1	*Add State-specific criteria for this business objective here.* *Example: Supports various authentication mechanisms, such as* ▪ *Biometric identification* ▪ *Password and/or personal identification numbers* ▪ *Telephone callback procedure* ▪ *Tokens (hard token, soft token, one time password devise token)* ▪ *Registration and identity proofing (digital signatures)*				

SP2– PROTECT THE CONFIDENTIALITY AND INTEGRITY OF ePHI					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP2.1	Contains verification mechanisms that are capable of authenticating authority (as well as identify) for the use or disclosure requested. For example: ▪ Denies general practitioner inquiry for recipient eligibility for mental health services ▪ Permits inquiries on claim status only for claims submitted by the inquiring provider	CFR			
SP2.2	Supports encryption and decryption of stored ePHI or an equivalent alternative protection mechanism.	CFR			

PROGRAM MANAGEMENT BUSINESS AREA
SECURITY AND PRIVACY (SP) CHECKLIST

SP2– PROTECT THE CONFIDENTIALITY AND INTEGRITY OF ePHI					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP2.3	Supports encryption of ePHI that is being transmitted, as appropriate.	CFR			
SP2.4	Supports integrity controls to guarantee that transmitted ePHI is not improperly modified without detection (e.g., provide secure claims transmission).	CFR			
SP2.5	Provides data integrity of ePHI by preventing and detecting improper alteration or destruction (e.g., double keying, message authentication, digital signature, check sums etc).	CFR			
SP2SS.1	*Add State-specific criteria for this business objective here.*				

SP3 – MONITOR SYSTEM ACTIVITY AND ACT ON SECURITY INCIDENTS					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP3.1	Provides the capability that all system activity can be traced to a specific user.	IBP			

PROGRAM MANAGEMENT BUSINESS AREA
SECURITY AND PRIVACY (SP) CHECKLIST

SP3 – MONITOR SYSTEM ACTIVITY AND ACT ON SECURITY INCIDENTS					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP3.2	Generates alerts for conditions that violate security rules, for example: ▪ Attempts to access unauthorized data and system functions ▪ Logon attempts that exceed the maximum allowed ▪ Termination of authorized sessions after a specified time of no activity	CFR			
SP3.3	Logs and examines system activity in accordance with audit polices and procedures adopted by the Medicaid agency.	CFR			
SP3.4	Provides security incident reporting and mitigation mechanisms, such as: ▪ Generate warning or report on system activity based on security parameters ▪ Terminate access and/or generate report when potential security violation detected ▪ Preserve and report specified audit data when potential security violation detected	CFR			
SP3.5	Supports procedures for guarding, monitoring, and detecting malicious software (e.g., viruses, worms, malicious code, etc.).	CFR			
SP3SS.1	*Add State-specific criteria for this business objective here.*				

PROGRAM MANAGEMENT BUSINESS AREA
SECURITY AND PRIVACY (SP) CHECKLIST

SP4 – SUPPORT INDIVIDUAL RIGHTS					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SP4.1	Has the capability to respond to an authorized request to provide a report containing the DRS for a given individual.	CFR			
SP4.2	Contains indicators that can be set to restrict distribution of ePHI in situations where it would normally be distributed.	CFR			
SP4.3	Tracks disclosures of ePHI; provides authorized users access to and reports on the disclosures.	CFR			
SP4.4	Has the capability to identify and note amendments to the DRS for a given individual.	CFR			
SP4SS.1	*Add State-specific criteria for this objective here.*				

SPSS1 – FIRST STATE-SPECIFIC BUSINESS OBJECTIVE					
Ref #	**System Review Criteria**	**Source**	**Yes**	**No**	**Comments**
SPSS1.1	*Add criteria based on the APD, RFP, etc., that are relevant to this State-specific objective*.				