Technical Support Services<br>for the Medicaid<br>HIPAA-Compliant<br>Concept Model<br>(MHCCM)

# Project Management Checklist Tool for the HIPAA Privacy Rule

## A Risk Assessment Checklist for Medicaid State Agencies

**Version 1.1**

**June 26, 2002**

**Prepared for:**
**Centers for Medicare & Medicaid Services**
**Center for Medicaid and State Operations**
**7500 Security Boulevard**
**Baltimore, MD 21244 – 1850**

# PROJECT MANAGEMENT CHECKLIST TOOL for the HIPAA PRIVACY RULE (MEDICAID AGENCY SELF-ASSESSMENT)

This risk assessment checklist is provided as a self-assessment tool to allow State Medicaid agencies to gauge where they are in the overall picture of HIPAA Privacy project implementation. This checklist is intended to be used by the HIPAA Privacy Coordinator/ Project Lead, or other key agency representative in the Medicaid agency in their role as the privacy project manager. The checklist does not interpret the privacy rule. **THE DHHS OFFICE OF CIVIL RIGHTS (OCR) IS THE DESIGNATED AUTHORITY REGARDING INTERPRETATIONS, IMPLEMENTATIONS AND ENFORCEMENT OF THE RULE.** The OCR website address for all information about the privacy rule is: **http://www.hhs.gov/ocr**. Use of this checklist is voluntary; it is intended to assist the agency and is not required to be submitted to CMS. Other State agencies could use this checklist but might need to modify some of the questions.

The "Yes" column following each item can be checked if the person completing it can respond positively to the question i.e., the item is completed or in progress. The "Yes" column can also be checked if adequate resources and planning have been allocated for future efforts. If these criteria are not met, the "No" column should be checked.

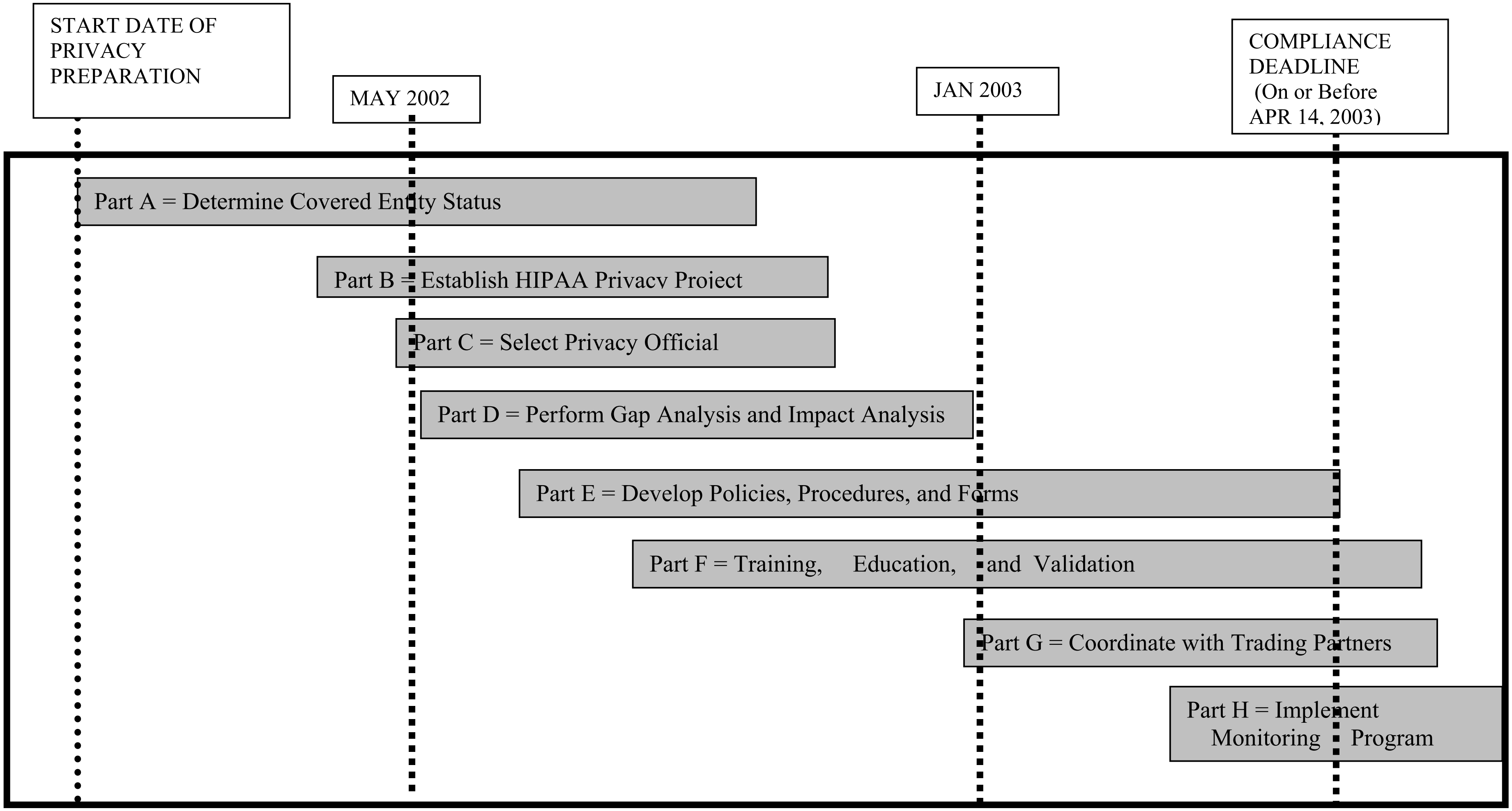
There are no official score sheets or right or wrong answers; the list of questions is provided as an aid to help establish a measure of progress and highlight work still needing to be accomplished. The list is also intended to provide ideas on areas that States or agencies may not have considered in their project efforts toward HIPAA compliance. It is in the organization's best interest to answer the questions as honestly and accurately as possible. The HIPAA privacy project manager is usually in the best position to provide accurate answers to the questions and can act as the best judge of the status of each project area in the checklist.

**Each question for which a "No" answer was supplied should be examined, and the reason for which "No" was given should be understood. If the "No" answer is appropriate for the activities required to become HIPAA compliant, it need not be considered further and "N/A" can be put in the answer boxes. The checklist is intended to serve as a tool for identifying areas of project risk. Every "No" answer remaining after the analysis is an indication of an area of risk. The more remaining "No's", the higher the risk for achieving Privacy compliance. In general, the project is at low risk if the answers are mainly "Yes" or "N/A". However, even in the case of many "No" responses to the questions, this checklist is <u>not</u> intended to give the impression that the organization is not going to successfully achieve HIPAA compliance. The results of the self-assessment should allow better focus of organization efforts in the time remaining until April 14, 2003.**

Please be aware that this checklist only applies to the Privacy Rule. The Transactions and Code Sets (TCS) Rule must also be implemented during this time period. Activities pertaining to TCS are <u>not</u> included in this checklist. There is a separate project management checklist tool available for TCS.

The timeline graphic illustrates the overlapping of project phases and activities and the overall chronology of project activity. The timeline also provides comparison dates of May, 2002 and January 2, 2003 to provide a general indication of where each organization should be in the project timeline. This is a depiction of an "ideal project". Roughly, a Privacy Project can correlate its own timeline to this one by aligning its actual start date with this timeline's start date and then comparing its tasks and activities with the timeline for the 8 defined project areas (A-H).

# PLOTTING THE PRIVACY PROJECT TIMELINE



START DATE OF PRIVACY PREPARATION

MAY 2002

JAN 2003

COMPLIANCE DEADLINE (On or Before APR 14, 2003)

Part A = Determine Covered Entity Status

Part B = Establish HIPAA Privacy Project

Part C = Select Privacy Official

Part D = Perform Gap Analysis and Impact Analysis

Part E = Develop Policies, Procedures, and Forms

Part F = Training, Education, and Validation

Part G = Coordinate with Trading Partners

Part H = Implement Monitoring Program

# PROJECT MANAGEMENT CHECKLIST TOOL for the HIPAA PRIVACY RULE
# (A Risk Assessment Checklist for Medicaid State Agencies)

## Checklist Contents

## Part A – Determine Covered Entity Status

### 1. Determine Covered Entity Status

*Determining covered entity status is the first step on the road to HIPAA Privacy compliance.*

| | Yes | No |
|---|---|---|
| Has the Medicaid agency reviewed each entity it administers based upon the Privacy Regulation? | | |
| Has the Covered Entity status based on the Privacy Regulation been determined for each entity? | | |
| If the Covered Entity status is "hybrid" (for Privacy), has the Covered Entity (or Medicaid agency) defined the included and excluded components? | | |
| If the Covered Entity status is "hybrid" (for Privacy), has the Covered Entity (or Medicaid agency) defined fire walls to separate the excluded components? | | |

# Part B – Establish Medicaid HIPAA Privacy Project

## 2. Establish a Medicaid HIPAA Privacy Project Office

*The HIPAA Privacy Project Office can be Statewide or can be more specific to the covered entities. Responsibilities, structure, tasks, schedule, tracking, and reporting must be set up consistent with the location of the Office.*

| | Yes | No |
|---|---|---|
| Is a HIPAA Privacy Project Office (HPPO) established? | | |
| Does the HPPO have support at the highest State executive levels? | | |
| Is there a current Organization chart and Charter document for the HPPO? | | |
| Is the HPPO Lead required to periodically report the project status to State Senior Management? | | |

## 3. HIPAA Privacy Project Work Plan

*The Project Office must have a work plan that shows all activities needed to attain compliance. If there are subordinate entities, they may need their own plans, coordinated with the master HPPO plan.*

| | Yes | No |
|---|---|---|
| Is there a HIPAA Privacy Project Work Plan? | | |
| If needed, are there subordinate work plans for subordinate entities? | | |
| Are reasonable timelines established for critical activities? | | |
| Are specific individuals responsible for updating the plan? | | |
| Does the plan include outreach activities to business associates? | | |
| Has the latest Privacy NPRM been analyzed to determine its impact on the plan? | | |

## 4. HIPAA Privacy Project Budgets, Resources, and Contracts

*Resources must be identified and available to complete identified tasks in the work plan.*

| | Yes | No |
|---|---|---|
| Does the HPPO have a budget for HIPAA Privacy compliance? | | |
| Is there a resource plan? | | |
| Are the staffing requirements assessed for the entire duration of the project? | | |
| Are staffing resources available when needed? | | |
| Does the HPPO have a firm commitment of resources and staff to meet its requirements? | | |
| Are the necessary services and support contracts in place? | | |

## 5. Security Implications

*Even though the Security Standard has not been signed, adequate security to protect health information is required to assure privacy.*

| | Yes | No |
|---|---|---|
| Has the HPPO identified security requirements needed for Privacy compliance? | | |
| Has the HPPO assessed current security capabilities and processes? | | |
| If needed, is there a plan to enhance security capabilities and processes to support Privacy requirements? | | |

## 6. Scheduling and Tracking Project Activities

*Individual plans and schedules should be tracked for the renovation effort.*

| | Yes | No |
|---|---|---|
| Do HPPO schedules define tasks and milestones, indicating responsible entities and dependencies? | | |
| Are there processes and tools to support maintaining project plans and schedules? | | |
| Is a process for identifying, reporting, tracking, and monitoring all issues to resolution in place? | | |
| Does this process include a mechanism for resolution of issues that arise between organizational entities? | | |
| Do all subordinate entities report to the HPPO on progress? | | |
| Is there periodic State executive level review of progress and deadlines? | | |

## Part C – Identify a HIPAA Privacy Official

### 7. Recruit and Hire a HIPAA Privacy Official

*Each covered entity must name a Privacy Official. Multiple entities may name the same Official, if this is suitable for the organizational structure. The HIPAA Privacy Official needs to have a level of authority consistent with the level of covered entity status.*

| | Yes | No |
|---|---|---|
| Has a HIPAA Privacy Official been named for each covered entity? | | |
| Is the HIPAA Privacy Official position at a level consistent with the range of responsibilities associated with the Covered Entity? | | |
| Does the Privacy Official have dedicated staff (direct or contracted)? | | |

### 8. Define the Privacy Official role

*The Privacy Official has a role defined in the Federal law. The job description needs to be consistent with this level of responsibility.*

| | Yes | No |
|---|---|---|
| Have the Privacy Official's responsibilities been documented? | | |
| Has legal counsel ruled on the adequacy of the documented role? | | |
| Does the Privacy Official have authority to carry out the directives of the role (i.e., to impose Privacy policies and procedures throughout the covered entity)? | | |

## Part D – Perform Gap Analysis and Measure Impact on Medicaid Facilities, Systems, and Business Processes

### 9. Perform Gap Analysis

*If the State statutes are demonstrated to be more restrictive than the Federal regulation, the State laws will take precedence. Burden of proof is on the State.*

| | Yes | No |
|---|---|---|
| Has the HIPAA Privacy regulation been compared (cross walked) with all relevant State privacy and confidentiality statutes? | | |
| Has the State determined whether or not the State statutes are more restrictive than the Federal? | | |
| Has there been a legal opinion given on the status of State statutes? | | |
| Have the total set of privacy requirements (Federal, State, entity) been documented? | | |

| | | |
|---|---|---|
| Have the gaps between requirements and current Privacy status been analyzed? | | |
| Is there a method, such as a questionnaire, to assess Privacy gaps across all covered organizational entities? | | |
| Was the questionnaire widely distributed to all levels of staff in all entities? | | |
| Were the responses captured for analysis? | | |
| Does the questionnaire cover all requirements of the Privacy Regulation? | | |
| Has the privacy gap analysis been updated and finalized based on survey results? | | |

## 10. Identify Impact, Review, and Re-Engineer Business Processes

*Business Processes must be assessed for HIPAA Privacy impact and prioritized for re-engineering (requiring changes in policy, procedures, training, and use of data).*

| | Yes | No |
|---|---|---|
| Have Medicaid business functions been inventoried? | | |
| Has the inventory been verified against the business functions identified in the MHCCM Operations Perspective? | | |
| Have the business processes been assessed for Privacy impact? | | |
| Have the required changes been developed and documented? | | |
| Can all impacted business processes be ready by the Privacy compliance date? | | |
| Are all facility or locations impacted by the Privacy rule been identified? | | |
| Are building or space modifications required? | | |
| Have all information systems and communications networks that store, maintain, or transmit PHI been identified? | | |
| Can the information systems implement the security and process requirements needed for Privacy compliance? | | |

# Part E – Develop Privacy Policies, Procedures, and Forms

## 11. Identify Policies, Procedures, and Forms that Need to Be Developed for Privacy

*Developing and deploying Privacy policies and procedures is at the heart of meeting compliance requirements. It can be a significant, labor-intensive undertaking.*

| | Yes | No |
|---|---|---|
| Is there a standard process to manage/oversee development of policies and procedures for Privacy? | | |
| Have current policies and procedures been compared to HIPAA Privacy requirements? | | |
| Has the agency developed information practices statement, consent, and authorization forms and policies for their use in accordance with HIPAA standards? | | |
| Is there a list of all procedures required by the HIPAA Privacy Rule? | | |
| Have the procedures for release and disclosure of health information been compared to each of the following HIPAA privacy standards: | | |
| 164.530(a) Standard: Personnel Designations | | |
| 164.502(b) Standard: Minimum Use and Disclosure of PHI | | |
| 164.530(b) Standard: Training | | |
| 164.530(c) Standard: Safeguards | | |
| 164.530(d) Standard: Complaints to the Covered Entity | | |
| 164.530(e) Standard: Sanctions | | |
| 164.530(f) Standard: Mitigation | | |
| 164.530(g) Standard: Refraining from Intimidating or Retaliatory Acts | | |
| 164.530(h) Standard: Waiver of Rights | | |
| 164.530(i) Standard: Policies and Procedures | | |
| 164.530(j) Documentation | | |
| Have changes to existing policies and procedures for each standard been identified? | | |
| Has the agency identified new policies and procedures needed to ensure all HIPAA requirements are met? | | |
| Is there an approval process for policies and procedures? | | |
| Is there a plan to update policies and procedures with regulatory changes or at periodic intervals? | | |

## Part F – Training, Education, and Validation

### 12. Develop and Implement Staff Training and Education Program

*For Privacy to be successfully implemented, all staff must be trained in the policies and procedures.*

| | Yes | No |
|---|---|---|
| Have all staff that need training in Privacy policy and procedures been identified? | | |
| Is there a training plan to reach all identified employees? | | |
| Does the training program include a course curriculum, training materials, and periodic updates? | | |
| Is the training plan geared to target different business functions and different staff job descriptions? | | |
| Has the training program been implemented? | | |
| Has the training program been reviewed by legal counsel? | | |
| Is there a privacy awareness process for employees other than those who will be directly trained? | | |

### 13. Validation

*Training and Education programs must be validated for effectiveness.*

| | Yes | No |
|---|---|---|
| Is there a plan to validate the effectiveness of staff training? | | |
| Is there a process to correct deficiencies found as a result of inadequate staff training? | | |
| Have new or re-engineered business processes affected by Privacy, and related policies and procedures been validated? | | |
| Have the system changes related to Privacy been tested? | | |
| Are procedures in place to retrain and retest when Privacy procedures are changed? | | |

# Part G – Coordinate with Data Trading Partners

## 14. Outreach to Business Partners

*Inclusion of the State Medicaid Enterprise. For guidance, see the CMS paper "*OUTREACH TO DATA TRADING PARTNERS*: "You're OK, I'm OK*"".

| | Yes | No |
|---|---|---|
| Is there a Privacy Outreach Plan for business associates and trading partners? | | |
| Has the agency identified all business associates and trading partners to be included in the outreach efforts? | | |
| Has a survey been sent to providers to determine their HIPAA Privacy compliance status? | | |
| Are providers able to send and receive encrypted data? | | |

## 15. Agreements

*Trading Partner agreements need to be updated for Privacy.*

| | Yes | No |
|---|---|---|
| Has language regarding mutual Privacy provisions been evaluated for addition to Trading Partner agreements? | | |
| Have all Trading Partners whose agreements should contain privacy provisions been identified? | | |
| Was legal counsel involved in developing the contract language and changes? | | |
| Has it been determined what protected health information is provided to which partners and that it is appropriate for the business purposes? | | |
| Is there a process for developing contract amendments as necessary to meet HIPAA requirements to safeguard protected health care information? | | |
| Are the contracts filed in a secure place? | | |
| Have all business associate contracts been examined in light of the Privacy Regulation? | | |
| Have all appropriate sections of these contracts been updated or rewritten to ensure HIPAA Privacy compliance? | | |

## Part H – Implement Monitoring Program

### 16. Develop and Implement a Monitoring and Oversight Program

*A covered entity should conduct internal oversight and monitoring to assure ongoing compliance with Privacy.*

| | Yes | No |
|---|---|---|
| Is there a plan and designated resources for ongoing oversight and maintenance necessary to remain in compliance with the Privacy rule, e.g., the Privacy official and other staff? | | |
| Is there a process and designated resources for the resolution of issues and handling of complaints, e.g., the Privacy official and other staff? | | |
| Is there an auditing function to determine staff compliance with HIPAA privacy requirements? | | |
| Has this function been staffed and are auditors trained? | | |
| Does the audit function have a budget? | | |
| Has the audit program been reviewed by legal counsel? | | |

### 17. Develop and Implement a Process for Corrective Action

*Corrective Action may be necessary to maintain compliance with Privacy.*

| | Yes | No |
|---|---|---|
| Is there a plan and dedicated resources to investigate and respond to audit findings? | | |
| Is there a process and designated resources to implement corrective actions? | | |