CENTERS for MEDICARE & MEDICAID SERVICES

Project Management Checklist Tool for the HIPAA Privacy Rule

A Risk Assessment Checklist for Medicaid State Agencies

Checklist Information

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

"Yes" Criteria

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 or if the question does not apply to your system or agency. If these criteria are not met, the “No” column should be checked.

Using the Checklist

Scroll through the sections and answer each question by clicking on the "yes" or "no" boxes according to the criteria defined in the above paragraph. There is a color-coded cell in the header of each section that will change color according to the risk associated with that section. Green equals low risk, yellow equals moderate risk, and red equals high risk. When all sections have been completed, you may scroll back through the Data Input worksheet to scan for the color coded tabs, or proceeed to the results worksheet by clicking on the corresponding "Results" tab at the bottom of this worksheet.

Results

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.

then combined to produce a score for that section. The "Results" worksheet provides a presentation of the scores for each section in bar grapg and color-coded table formats. Very low scores indicate areas of probable high risk. High scores do not indicate no risk, rather areas of the project that, based on the answers provided, do not pose an immediate risk for the project.

“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

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.

Help

For technical assistance with this checklist you may contact Bob Guenther (robert.guenther@titan.com). For general questions, or for more information regarding the tool you may contact Henry Chao in the CMS Central Office (hchao@cms.hhs.gov).

HIPAA Privacy Rule Risk Assessment Checklist

Part A – Determine Covered Entity Status

1.0 Determination of Covered Entity Status	
Has the State reviewed each entity it administers based upon the Privacy Regulation?	□ YES □ NO
Has the State Covered Entity Status based on the Privacy Regulation been determined for each entity?	□ YES □ NO
If the covered entity status is "Hybrid" (for Privacy), has the covered entity (or Medicaid agency) defined the included and excluded components?	□ YES □ NO
If the covered entity status is "Hybrid" (for Privacy), has the covered entity (or Medicaid agency) defined firewalls to separate the excluded components?	□ YES □ NO

Part B - Establish Medicaid HIPAA Privacy Project

2.0 Establishment of a Medicaid HIPAA Privacy Project Office	
Is a HIPAA Privacy Project Office (HPPO) established?	□ YES □ NO
Does the HPPO have support at the highest State executive levels?	□ YES □ NO
Is there a current Organization chart and Charter document for the HPPO?	□ YES □ NO
Is the HPPO Lead required to periodically report the project status to State Senior Management?	□ YES □ NO

3.0 HIPAA Privacy Project Work Plan

Is there a HIPAA Privacy Project Work Plan? □ YES □ NO

If needed, are there subordinate work plans for subordinate entities? □ YES □ NO

Are reasonable timelines established for critical activities? □ YES □ NO

Are specific individuals responsible for updating the plan? □ YES □ NO

Does the plan include outreach activities to business associates? □ YES □ NO

Has the latest Privacy NPRM been analyzed to determine its impact on the plan? □ YES □ NO

4.0 HIPAA Privacy Project Budgets, Resources, and Contracts

Does the HPPO have a budget for HIPAA Privacy compliance? □ YES □ NO

Is there a resource plan? □ YES □ NO

Are the staffing requirements assessed for the entire duration of the project? □ YES □ NO

Are staffing resources available when needed? □ YES □ NO

Does the HPPO have a firm commitment of resources and staff to meet its requirements? □ YES □ NO

Are the necessary services and support contracts in place? □ YES □ NO

5.0 Security Implications

Has the HPPO identified security requirements needed for Privacy compliance? □ YES □ NO

Has the HPPO assessed current security capabilities and processes? □ YES □ NO

If needed, is there a plan to enhance security capabilities and processes to support Privacy requirements? □ YES □ NO

6.0 Scheduling and Tracking Project Activities

Do HPPO schedules define tasks and milestones, indicating responsible entities and dependencies? □ YES □ NO

□ YES □ NO

Are there processes and tools to support maintaining project plans and schedules?	□ YES □ NO
Is a process for identifying, reporting, tracking, and monitoring all issues to resolution in place?	□ YES □ NO
Does this process include a mechanism for resolution of issues that arise between organizational entities?	□ YES □ NO
Do all subordinate entities report to the HPPO on progress?	□ YES □ NO
Is there periodic State executive level review of progress and deadlines?	□ YES □ NO

Part C – Identify a HIPAA Privacy Officia 🟥

7.0 Recruit and Hire a HIPAA Privacy Official

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

8.0 Define the Privacy Official role

Have the Privacy Official's responsibilities been documented?	□ YES □ NO
Has legal counsel ruled on the adequacy of the documented role?	□ YES □ NO
Does the Privacy Official have authority to impose Privacy policies and procedures throughout the covered entity?	□ YES □ NO

Part D - Perform Gap Analysis and Measure Impact on Medicaid Facilities, Systems, and Business Processes 🟥

9.0 Perform Gap Analysis

Has the HIPAA Privacy regulation been compared (cross walked) with all relevant State privacy and confidentiality statutes?	□ YES □ NO

Has the State determined whether or not the State statutes are more restrictive than the Federal?	□ YES	□ NO
Has there been a legal opinion given on the status of State statutes?	□ YES	□ NO
Have the total set of privacy requirements (Federal, State, entity) been documented?	□ YES	□ NO
Have the gaps between requirements and current Privacy status been analyzed?	□ YES	□ NO
Is there a method, such as a questionnaire, to assess Privacy gaps across all covered organizational entities?	□ YES	□ NO
Was the questionnaire widely distributed to all levels of staff in all entities?	□ YES	□ NO
Were the responses captured for analysis?	□ YES	□ NO
Does the questionnaire cover all requirements of the Privacy Regulation?	□ YES	□ NO
Has the privacy gap analysis been updated and finalized based on survey results?	□ YES	□ NO

10.0 Identify Impact, Review, and Re-Engineer Business Processes

Have Medicaid business functions been inventoried?	□ YES	□ NO
Has the inventory been verified against the business functions identified in the MHCCM Operations Perspective?	□ YES	□ NO
Have the business processes been assessed for Privacy impact?	□ YES	□ NO
Have the required changes been developed and documented?	□ YES	□ NO
Can all impacted business processes be ready by the Privacy compliance date?	□ YES	□ NO
Have all facilities or locations impacted by the Privacy rule been identified?	□ YES	□ NO
Are building or space modifications required?	□ YES	□ NO
Have all information systems and communications networks that store, maintain, or transmit PHI been identified?	□ YES	□ NO

Can the information systems implement the security and process requirements needed for Privacy compliance?	□ YES □ NO

Part E - Develop Privacy Policies, Procedures, and Forms

11.0 Identify Policies, Procedures and Forms that Need to Be Developed for Privacy

Is there a standard process to manage/oversee development of policies and procedures for Privacy?	□ YES □ NO
Have current policies and procedures been compared to HIPAA Privacy requirements?	□ YES □ NO
Has the Agency developed information practices statement, consent, and authorization forms and policies for their use in accordance with HIPAA standards?	□ YES □ NO
Is there a list of all procedures required by the HIPAA Privacy Rule?	□ YES □ NO
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	□ YES □ NO
164.502(b) Standard: Minimum Use and Disclosure of PHI	□ YES □ NO
164.530(b) Standard: Training	□ YES □ NO
164.530(c) Standard: Safeguards	□ YES □ NO
164.530(d) Standard: Complaints to the Covered Entity	□ YES □ NO
164.530(e) Standard: Sanctions	□ YES □ NO
164.530(f) Standard: Mitigation	□ YES □ NO
164.530(g) Standard: Refraining from Intimidating or Retaliatory Acts	□ YES □ NO
	□ YES □ NO

164.530(h) Standard: Waiver of Rights	□ YES	□ NO
164.530(i) Standard: Policies and Procedures	□ YES	□ NO
164.530(j) Documentation	□ YES	□ NO
Have changes to existing policies and procedure for each standard been identified?	□ YES	□ NO
Has the agency identified new policies and procedures needed to ensure all HIPAA requirements are met?	□ YES	□ NO
Is there an approval process for policies and procedures?	□ YES	□ NO
Is there a plan to update policies and procedures with regulatory changes or at periodic intervals?	□ YES	□ NO

Part F - Training, Education, and Validation

12.0 Develop and Implement Staff Training and Education Program

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

13.0 Validation

□ YES □ NO

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

Part G - Coordinate with Data Trading Partners

14.0 Outreach to Business Partners

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

15.0 Agreements

Has language regarding mutual Privacy provisions been evaluated for addition to Trading Partner agreements?	□ YES	□ NO
Have all Trading Partners whose agreements should contain privacy provisions been identified?	□ YES	□ NO
Was legal counsel involved in developing the contract language and changes?	□ YES	□ NO
Has it been determined what protected health information is provided to which partners and that it is appropriate for the business purposes?	□ YES	□ NO
Is there a process for developing contract amendments as necessary to meet HIPAA requirements to safeguard protected health care information?	□ YES	□ NO

Are the contracts filed in a secure place?	□ YES □ NO
Have all business associate contracts been examined in light of the Privacy Regulation?	□ YES □ NO
Have all appropriate sections of these contracts been updated or rewritten to ensure HIPAA Privacy compliance?	□ YES □ NO

Part H - Implement Monitoring Program

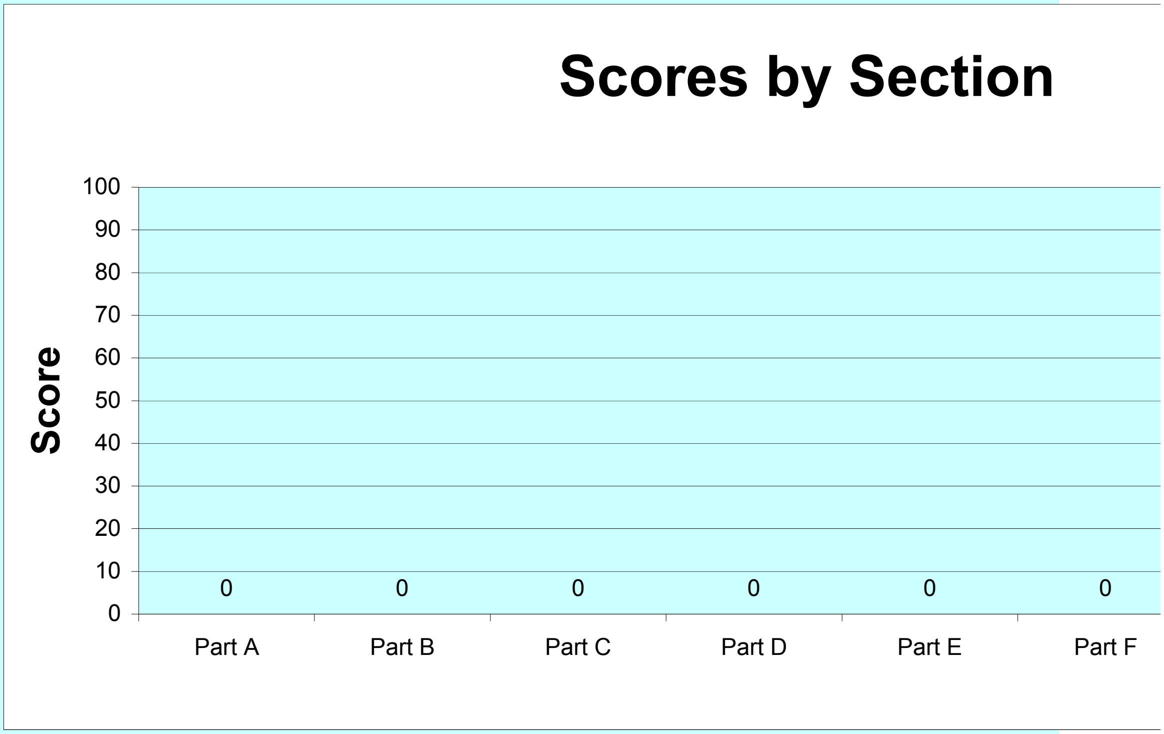
16.0 Develop and Implement a Monitoring and Oversight Program

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)?	□ YES □ NO
Is there a process and designated resources for the resolution of issues and handling of complaints (e.g., the Privacy official and other staff)?	□ YES □ NO
Is there an auditing function to determine staff compliance with HIPAA privacy requirements?	□ YES □ NO
Has this function been staffed and are auditors trained?	□ YES □ NO
Does the audit function have a budget?	□ YES □ NO
Has the audit program been reviewed by legal counsel?	□ YES □ NO

17.0 Develop and Implement a Process for Corrective Action

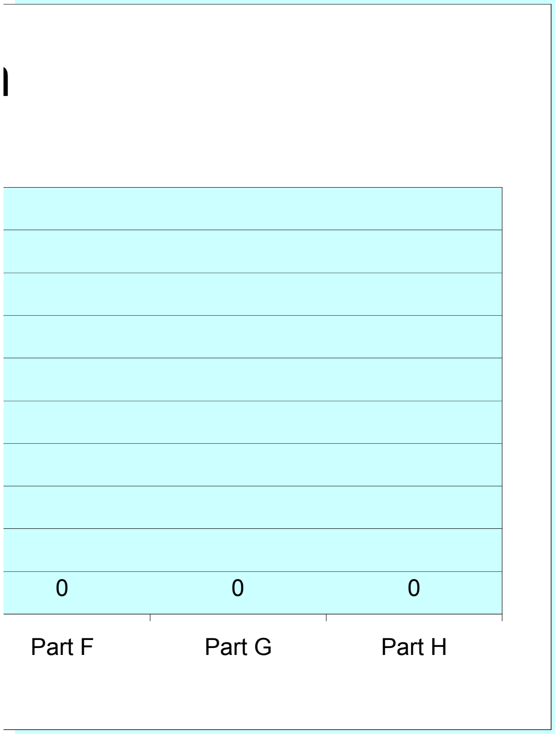
Is there a plan and designated resources to investigate and respond to audit findings?	□ YES □ NO
Is there a process and designated resources to implement corrective actions?	□ YES □ NO

Overall Self Assessment Score Is:	**0**



Risk by Section

Part A	Determine Covered Entity Status	🟥
Part B	Establish Medicaid HIPAA Privacy Project	🟥
Part C	Identify a HIPAA Privacy Official	🟥
Part D	Perform Gap Analysis and Measure Impact on Medicaid Facilities, Systems, and Business Processes	🟥
Part E	Develop Privacy Policies, Procedures, and Forms	🟥
Part F	Training, Education, and Validation	🟥
Part G	Coordinate with Data Trading Partners	🟥
Part H	Implement Monitoring Program	🟥


0
0
0
Part F
Part G
Part H