

<b>DEPARTMENT OF PERSONNEL &amp; ADMINISTRATION</b>		HIPAA Policy No.	4
		Current Effective Date	May 1, 2006
		Original Effective Date	May 1, 2006
<b>HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT</b>		Approved by: Jeffrey C. Schutt	
<b>RISK ANALYSIS /ASSESSMENT</b>		Date: 4/25/06	

**I. Purpose**

The HIPAA Security Rule requires the Department of Personnel and Administration (DPA) to assess the potential risks and vulnerabilities to its information systems containing electronic protected health information (ePHI). The purpose of this policy is to ensure that these systems are assessed on a regular basis.

**II. Policy**

Risk assessments of DPA systems containing ePHI shall be conducted every two (2) years (based on the State's fiscal year), and must be completed no later than October 31<sup>st</sup> of the scheduled year. These regularly scheduled biennial risk assessments will be conducted by an outside consulting firm and by DPA personnel, on an alternating basis. This will create a system of checks and balances. An outside consultant will conduct the risk assessment in Fiscal Year 2007.

Additional risk assessments may be conducted as circumstances require following significant environmental or operational changes that may affect the security of ePHI. DPA's Chief Information Officer (CIO) and HIPAA Compliance Officer (HCO) must approve any risk assessment conducted outside of the biennial cycle. An added risk assessment may preempt the next regularly scheduled risk assessment or change the risk assessment schedule. This decision will be made by DPA's CIO and HCO.

For all risk assessments, regardless of who performs them or when, a written report that includes findings, conclusions, and recommendations must be produced and provided to, at a minimum, DPA's CIO and HCO.

**III. Procedures**

- A. DPA's CIO will be responsible for all budget requests related to any risk assessment.
- B. DPA's CIO will be responsible for each selection through the procurement process of an outside consulting firm to conduct a risk assessment.
- C. For any risk assessment that will be conducted by DPA, DPA's CIO will designate appropriate personnel to carry out the task.
- D. Prior to the start on any risk assessment, DPA's CIO and HCO must be given a project plan that includes a timeline and responsible parties.
- E. For all risk assessments, regardless of who performs them or when, DPA's HCO must be kept informed of all major plans, decisions, and activities, including who will be conducting the risk assessment, starting date, ending date, progress, problems that occur along the way, findings, conclusions, and recommendations.

F. DPA's HCO will attend the initial planning meeting and the closing meeting for risk assessments that will be performed by DPA, and the entrance and exit conferences with the outside consultants for risk assessments that will be performed by outside consultants.

**IV. Definitions/Abbreviations**

None

**V. Revision History**

<u>Date</u>	<u>Description</u>
May 1, 2006	Original document

**VII. References/Citations**

<u>HIPAA Security Rule</u>	
45 CFR 164.308(a)(1)(i)	Security Management Process
45 CFR 164.308(a)(1)(ii)(A)	Risk Analysis