West Virginia Executive Branch

Privacy Impact Assessment Guidance

Issued by: West Virginia Health Care Authority

1.0 INTRODUCTION

The purpose of this document is to serve as an educational resource and best practices guide for all West Virginia Executive Branch Departments to efficiently and properly perform Privacy Impact Assessments (PIA). This guide illustrates when to conduct a PIA and the steps needed to support and assist Departments in PIA preparation and implementation activities.

2.0 BACKGROUND

The West Virginia Executive Branch privacy program balances an individual's right of privacy against others' need and right of access to personally identifiable information (PII). The West Virginia Executive Branch privacy program and policies are based upon these six privacy principles:

1. Accountability
2. Consent
3. Individual Rights
4. Minimum Necessary and Limited Use
5. Notice
6. Security Safeguards

Focusing on and managing privacy decreases the risk of unauthorized access to PII and fosters trust between the government and the citizens of the State. A PIA is used to assess the privacy impact and risks to PII stored, used and exchanged by information systems. A PIA evaluates privacy implications when information systems are created, when existing systems are significantly modified or when new technology is purchased. PIAs provide numerous benefits, such as:

- Providing a proactive approach to privacy management;
- Evaluating whether appropriate privacy protections and necessary mitigation or safeguards are present;
- Applying privacy requirements, complementing organization-wide compliance activities (e.g. HIPAA privacy, etc.);
- Enhancing current data inventories of information collected, used, stored and exchanged by systems; and
- Providing opportunity for additional education and awareness about privacy.

3.0 WHEN TO CONDUCT A PIA

To be effective, a PIA should be an integral part of the project planning process. A PIA should be conducted to evaluate information privacy and security throughout the life cycle of a system, product or project and when sharing or exchanging PII with other organizations or Departments. Therefore, a Department should: a) start early to ensure that project risks are identified and appreciated before the problems become embedded in the design; b) incorporate a PIA into the project initiation phase); or c) if the project is already under way, start today, so that any major issues are identified with minimum possible delay.

Examples of activities which may trigger a PIA:

Conversions	• Converting paper-based records with PII to electronic records.
Significant System Management Changes and System Merging	• New uses of existing IT systems, including the application of new technologies and significant changes in how PII is managed in the system. For example, when a Department employs new relational database technologies or web-based processing to access multiple data stores, such additions could create avenues for exposure of PII that previously did not exist. • Agencies adopt or alter business processes so that Department databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such aggregation may create new privacy concerns.
Access	• New public access to a system.
Transferring	• Departments working together on new interagency uses or exchanges of PII.
Collection	• Departments developing, buying or contracting for new information technology systems to handle the collection of PII. • Collecting/adding new PII that raises the risk to personal privacy, such as adding health data.
Procurement	• Procuring new technologies or systems that will collect, use or store PII.

When a Department wishes to purchase new technology, Chief Technology Officer (CTO) approval is required. If the CTO determines the purchase has privacy implications and that a PIA has not been completed, the West Virginia Office of Technology will notify the Department Privacy Officer (DPO) and the State Privacy Office of the planned procurement. The DPO will contact the system owner or the project manager to ensure a PIA is completed. The DPO will also track this information on the agency vendor list.

4.0 PIA PROCESS

A web-based PIA questionnaire will be used to document and generate the PIA report. The PIA questionnaire provides a quick assessment for further analysis of risks and mitigation necessary to protect PII. The following chart details the process:

STEPS		**ROLES**	**PROCESS**
1	Identify the need for a PIA.	System Owner and/or Program Manager	Using the PIA tool, complete a Privacy Threshold Analysis to determine if PII is processed by any of the system's components. If answers to the qualifying questions are all NO, then a PIA is not warranted. If any of the answers are YES, go to step 2.
2	Describe the project's information flows.	System Owner and/or Program Manager	Complete PIA Questionnaire. Note: The system owner or program manager who completes the PIA will receive an email with the final report attached. A copy of the final report will auto-generate via email to the DPO and the State Privacy Office.
3	Identify privacy risks.	DPO	Review PIA report to identify privacy risks from the information provided. The DPO will collaborate with the System Owner and/or Program Manager to ensure compliance with privacy policies. If no privacy risks are identified, the PIA report should be retained per Department retention requirements. If there are any privacy risks, continue with steps 4 and 5.
4	Identify and evaluate privacy solutions.	System Owner and/or Program Manager and DPO	All parties should reach an agreement on the resolution of identified privacy or security risks. Reference Section 5.0 of this guidance.
5	Report assessment and resolution of privacy risks.	System Owner and/or Program Manager and DPO	A completed summary report of identified risks and resolution(s) should be completed and submitted to the Cabinet Secretary, Security Officer, and the State Privacy Office. Reference Section 5.0 of this guidance.

5.0 IDENTIFYING AND EVALUATING PRIVACY RISK SOLUTIONS

When privacy risks are identified, the DPO, security officer, and system owner should work together to develop recommendations for mitigation. However, there may be some risks that cannot be eliminated, and consideration should be given to escalating these risks to Department leadership. Below is a table showing an example of a risk evaluation, along with examples of identified risks, description of the risks, some possible measures for mitigation and which privacy policies relate to the risks.

EXAMPLE RISK EVALUATION:

The PIA identified seven potential privacy risks: Unauthorized Access; Data Collection; Use; Storage; Disclosure; Vendor; and Administrative, Physical and Technical Controls. Below is a summary of the risks identified, a brief description, solutions, mitigation measures and relevant privacy policies.

PRIVACY RISK	DESCRIPTION	RISK SOLUTIONS/ MITIGATION PLAN	PRIVACY POLICIES
Unauthorized Access	Snooping by users.	Ensure that there are access controls, training, confidentiality agreements and audit logs.	Accountability, Security Safeguards
Data Collection	PII will be collected without a clear purpose which could violate the privacy notice.	Ensure that there is a clearly identified and documented purpose for the collection and use of the PII, consistent with the privacy notice.	Minimum Necessary & Limited Use, Consent, Individual Rights, Notice
Use	Unsure of legal authority to collect/use the data collected.	Review the Privacy Requirements document and/or seek legal guidance.	Accountability, Minimum Necessary & Limited Use
Storage	Unsure of retention and destruction policies related to this project.	Review your Department's document retention policies.	Accountability, Minimum Necessary & Limited Use, Security Safeguards
Disclosure	Disclosure of PII to unauthorized recipients.	Identify and review how users plan to disclose/share data.	Minimum Necessary & Limited Use, Notice, Security Safeguards
Vendor	Health information will be disclosed to vendor.	Evaluate whether the vendor should also sign a HIPAA Business Associated Agreement.	Accountability, Minimum Necessary & Limited Use
Administrative, Physical and Technical Controls	There is a risk of intentional or unintentional breach by administrators with access to end user data.	Complete a security risk assessment, ensure security training, execution of confidentiality agreements and periodic auditing.	Accountability, Security Safeguards