

Exempt from FOIA¹

2008 West Virginia Executive Branch Data Assessment

A report by the State Privacy Office
West Virginia Health Care Authority
September, 2008

¹ Not for public release. Includes attorney client privileged information and internal analysis involving privacy and security issues - consult an attorney for assistance in asserting FOIA exemption.

Introduction

State government utilizes and discloses more Personally Identifiable Information (PII) than ever before. The State of West Virginia's unprecedented commitment, through the leadership of Governor Manchin, in protecting the confidentiality of PII collected and maintained by Executive Branch departments² exemplifies the State's concern in upholding the value of privacy. Thus, to obtain a more precise understanding of Executive Branch department practices regarding how PII is collected, stored, protected, shared and managed, a privacy data assessment was conducted. The information contained in this report discusses the current state of Executive Branch department privacy practices, before the issuance of Executive Branch-wide privacy policies.

This report can be utilized in assisting Executive Branch departments in better understanding areas where improvement may be needed in the area of protecting PII. Understanding information exchanges and data flow assists each Executive Branch department in distinguishing information that will be the subject of privacy policy and procedure development efforts. Furthermore, the assessment will assist each department in more fully understanding the information that it manages in order to identify data that require privacy protection.

Purpose

The overall purpose of the privacy data assessment is to identify how PII is collected, stored, protected, shared and managed. PII includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact (or impersonate) an individual. Examples include: individual's home address, phone and FAX numbers, credit and debit card numbers, mother's maiden name, Social Security Number, finger-print (s), Driver's License Number, full face photographic images, certificate numbers, medical record numbers, etc.

This report provides a high level summary of some of the assessment results.

Profile of Respondents

On average, 90 of the 143 respondents provided answers to the assessment questions. Respondents were chosen by means of department-level Privacy Officer selection, meaning, each department's Privacy Officer selected subdivisions within the department to participate in the assessment. The respondents consisted of Privacy Officials or their designee (133) and Legal Consultants or their designee (9) within the West Virginia Executive Branch.

The Assessment Tool

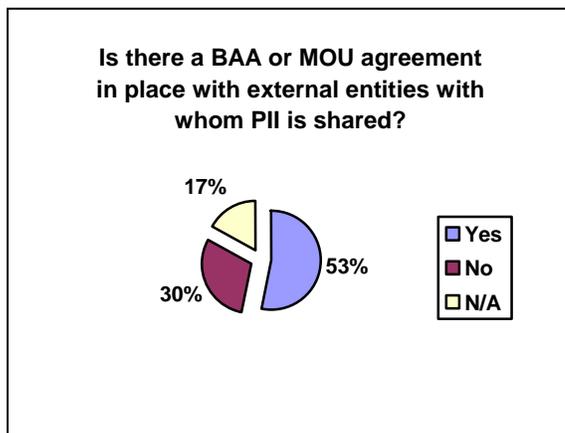
The Privacy Data Assessment Tool consisted of three main sections. The first section asked respondents to determine which data elements their department collected, stored, and disclosed. Section two of the assessment provided departments the opportunity to assess compliance with Executive Branch privacy principles which serve as the foundation of the privacy program's policies. Finally, in section three, each department's designated attorney or designee was asked to review each law and then make a determination of its application to their department.

² **Department:** A major division of the executive branch of state government that is responsible for administering a specific program area. As used in this report, a department includes its subdivision, bureaus, agencies, boards, commissions, councils, offices and other similarly situated entities.

Section One: Data Collection, Storage and Disclosure

The Privacy Management Team identified 24 PII data elements that the Executive Branch collects. As expected, the results show a high percent of PII being collected from the individual versus third parties. The results showed that the home address, phone number, Social Security Number (SSN) and birth date (age) were primarily collected. Respondents reported storing and disclosing PII in both paper and electronic format. Additional results show that PII is mostly disclosed within the department or between the department and other state government department. The major findings regarding “Data Collection, Storage and Disclosure” survey responses extracted from the study are:

- 83% of respondents used PII within their own department.
- 73% of respondents disclosed PII to other state departments.
- When asked if PII is disclosed externally (i.e. suppliers, vendors, customers, law enforcement), most of the respondents indicated “no”.
- 53% of the respondents reported having a Business Associate Agreement or a Memorandum of Understanding in place with external departments with whom PII is shared.



BAA or MOU Agreements can result in better privacy practices!

- ◆ BAA or MOU agreements allow for cooperation between departments concerning privacy related issues.
- ◆ BAA or MOU agreements assist departments in better addressing emerging privacy challenges and may enhance the management of cross-border privacy issues.
- ◆ BAA or MOU agreements help to ensure an ongoing high level of privacy protection regarding PII.

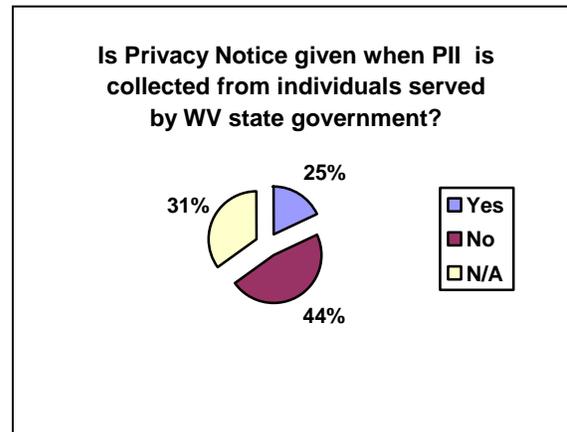
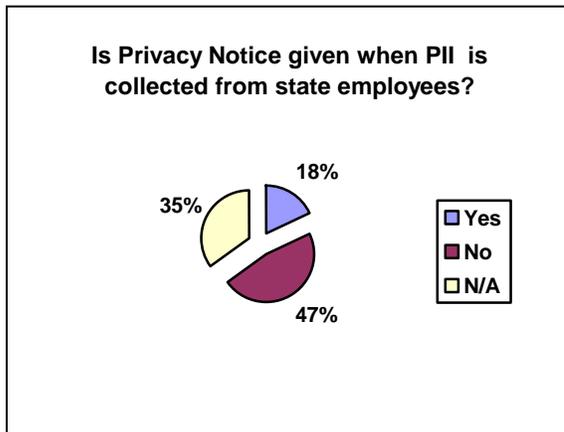
Section Two: Privacy Compliance

Section two of the assessment provided departments with the opportunity to assess compliance with Executive Branch privacy principles which serve as the foundation for the privacy program policies that will become effective Fall 2008; thus, this report will serve as the baseline. The privacy principles were adopted in July 2007.

Notice

Notice concerns an department’s openness regarding the authority for collecting PII; the purpose of the collection; the location of the department maintaining the PII; with whom the PII may be shared and why; rights an individual has in PII; and the department’s policies, procedures, standards, and practices with regard to PII. The major findings regarding “Notice” survey responses extracted from the study are:

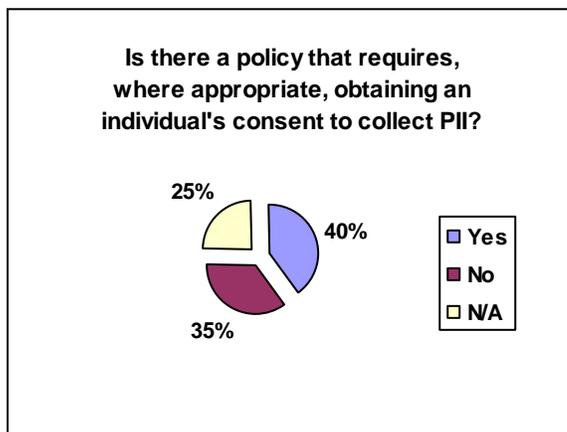
- 47% of respondents reported **NOT** giving state employees a privacy notice when PII was collected from employees.
- 44% of respondents reported **NOT** giving individuals served by WV state government a privacy notice when PII was collected from individuals.



Consent and Authorization

According to the Consent and Authorization principle, a department’s collection of personally identifiable information (PII) should be contingent upon first obtaining an individual’s consent to collection except when legally authorized to collect without permission. A department does not collect, use or disclose PII in a manner inconsistent with its notice, unless it has first obtained the individual’s permission for the use or disclosure. The major findings regarding “Consent and Authorization” survey responses extracted from the study are:

- 40 % of respondents reported having a policy that requires, where appropriate, obtaining an individual’s consent to collect PII.



Adhering to the Consent and Authorization principle can result in better privacy practices!

- ◆ The State must be accountable to the public regarding State collection of PII, unless legally authorized to collect without permission. Thus, adhering to the Consent and Authorization principle is of utmost importance in ensuring better privacy practices.

Individual Rights and Participation

Each Executive Branch department, when possible, relies first on the accuracy of the personally identifiable information (PII) including protected health information (PHI) it collects from the

individual, when an department believes the information is provided in good faith. The major findings regarding “Individual Rights and Participation” survey responses extracted from the study are:

- 62% of respondents reported that employees within their department are allowed to access their own PII. Furthermore, when asked if employees, which have access to their PII, have the ability to request that their PII be amended or modified, 61% of the respondents indicated “yes”.
- 45% of respondents reported that the public is allowed to access their own PII. Furthermore, when asked if the public, which have access to their PII, have the ability to request that their PII be amended or modified, 49% of the respondents indicated “yes”.

Another important aspect of Individual Rights and Participation principle involves departments having procedures which enable them to respond to individual complaints and appeals. The major findings regarding complaints/appeals procedures extracted from the study are:

- 63% of respondents reported that they **DO** have procedures in place enabling them to respond to individual complaints and appeals.
- 51% of the respondents reported that the procedures utilized in responding to individual complaints and appeals did include the handling of information privacy complaints.

Security Safeguards

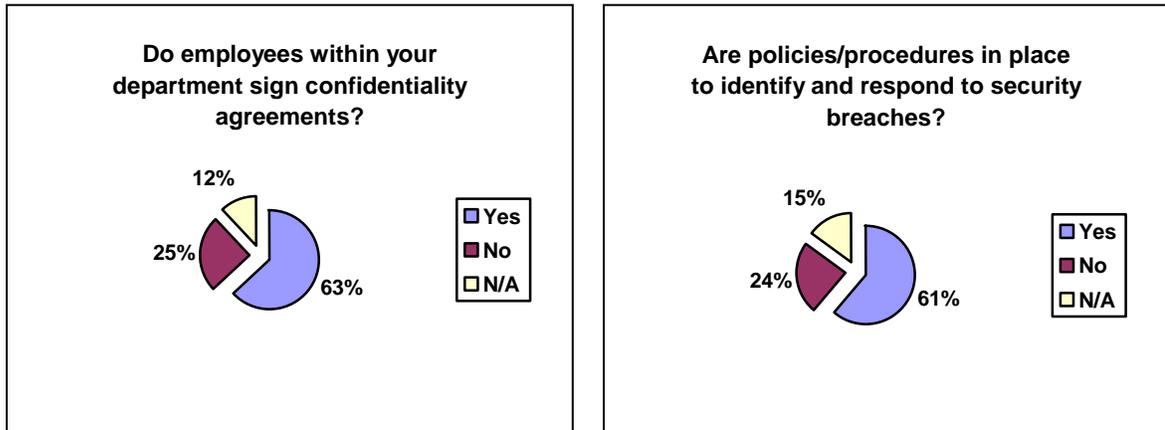
The Security Safeguards principle maintains that a department must implement appropriate management, operational and technical controls to preserve the privacy, confidentiality, integrity and accessibility of PII. The data shows that WV Executive Branch departments have fairly strong security safeguards for PII, such as procedures for revoking access to PII in a timely manner due to employee termination and/or occupation change. Furthermore, departments reported having appropriate password security measures in place. The major findings regarding “Security Safeguards” responses extracted from the study are:

- 61% of respondents reported having policies and procedures in place which enable them to respond to security breaches.
- 70% of respondents reported having procedures in place which verify the identity of individuals who access PII.
- 55% of respondents reported having procedures in place to identify and respond to unintended disclosure of PII.
- 63% of respondents reported that their department has procedures for securing PII data transmission internally (i.e. transmission via e-mail, telephone).
- 52% of respondents reported that they have procedures for securing PII data transmission externally (i.e. transmission via e-mail, telephone).

Security Safeguards are vitally important in protecting PII!

- ◆ It is often too late to prevent data breaches if a centralized security strategy is not in place to safeguard data.
- ◆ Without appropriate security, privacy of information cannot be maintained.

- 63% of respondents reported that employees of the department had signed confidentiality agreements.



Minimum Necessary and Limited Use

The Minimum Necessary and Limited Use principle states that collection, use, and disclosure of PII should be limited to an department’s legal authority and purpose, as set forth in an department’s notice. Overall, WV Executive Branch departments reported adhering to this principle. The major findings regarding “Minimum Necessary and Limited Use” survey responses extracted from the study are:

- 88% of respondents reported that when PII is collected, it is limited to the minimum necessary.
- 79% of respondents reported having policies and procedures which control an individual’s access to PII to that which is minimally necessary to complete the legally permitted task.

Accountability

The principle of Accountability designates each Executive Branch department as being responsible for maintaining the privacy of PII that it creates, stores or maintains within its possession or custody to the extent required by law. Managing this responsibility is the function of a designated privacy officer within each department. Moreover, each Cabinet Secretary designates a privacy officer who is accountable to the Secretary, the Chief Privacy Officer, and the Privacy Management Team in ensuring the application of the privacy policies to PII. The major findings regarding “Accountability” survey responses extracted from the study are:

- 94% of the respondents reported having a privacy official in place.
- 83% of respondents reported having a department-level privacy infrastructure in place, including privacy coordinators or contacts.

Privacy Requirements

There are over 30 federal and state privacy laws governing the Executive Branch’s collection, use, disclosure and retention of personally identifiable information (PII). Additionally, there may be specific laws or rules which govern the collection, use, disclosure and retention of PII for an

individual department which are not on the list. In section three, each department's designated attorney or designee was asked to review each law and then make a determination of its application to their department. The significance of this legal review is that, in the United States, a mixture of state and federal laws govern the privacy of information. Different laws, and thus, different requirements will be in play based upon the department collecting the information, as well as the information itself. Therefore, an understanding of the "rules" that govern an department's privacy program, over and above adopted privacy principles and policies, is essential for regulatory compliance. The federal laws with the highest impact were the Health Insurance Portability and Accountability Privacy Rule (HIPAA) and the Privacy Act. The state laws and or legal authorities with the highest impact were the Freedom of Information Act, W. Va. Code § 29B-1-1 *et seq.* and the Records Management and Preservation of Essential Records Act, W. Va. Code §§ 5A-8-21, 22.

Conclusion

This report is a high level summary of the assessment results concerning how PII is collected, stored, protected, shared and managed within Executive Branch departments. This assessment is one example of the many resources being utilized by the Privacy Management Team to ensure better privacy practices within the State of West Virginia. Overall, it can be reasoned from the data that Executive Branch departments do retain practices which support protecting the confidentiality of PII. However, there is area for improvement in regard to developing better privacy practices, particularly in the area of developing procedures to identify and respond to unintended disclosure of PII and in the area of obtaining, where appropriate, consent and authorization to collect an individual's PII. The issuance of Executive Branch Privacy Policies in Fall 2008 will further serve as a catalyst through which the State of West Virginia will continue its commitment to upholding the value of privacy for its employees and the citizens it serves.