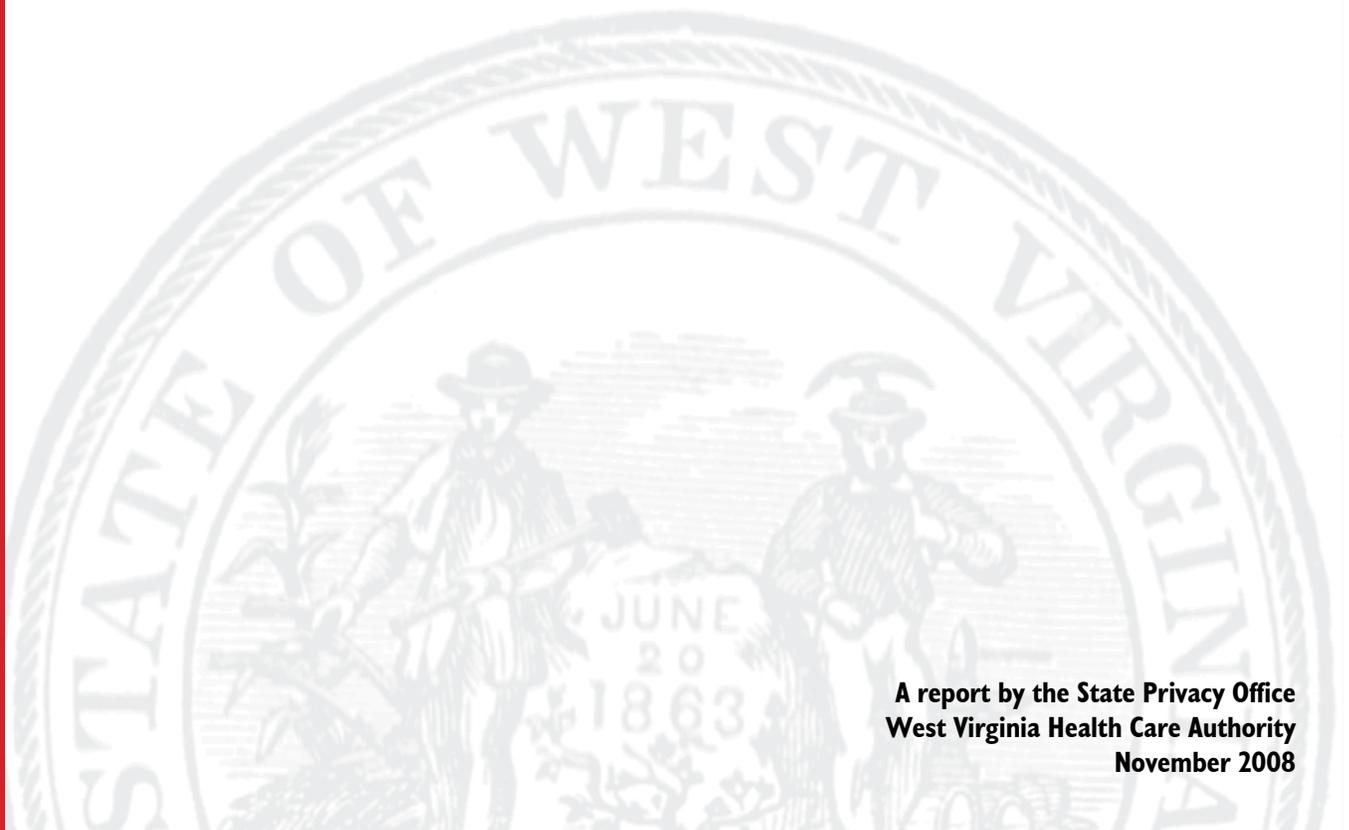




West Virginia State Privacy Office

2008 Annual Report



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

Executive Branch Departments

Governor's Office

Department of Administration

Department of Commerce

Department of Education & the Arts

Department of Environmental Protection

Department of Health and Human Resources

WV Health Care Authority

Department of Military Affairs & Public Safety

Bureau of Senior Services

Department of Revenue

Department of Transportation

Boards and Commissions

INTRODUCTION

The purpose of this annual report is to depict the Privacy Management Team's on-going activities concerning the advancement of processes being undertaken to protect the privacy of personally identifiable information (PII) collected and maintained by Executive Branch departments¹. Thus, the report will detail the major accomplishments of the Privacy Management Team as well as address new initiatives the Privacy Management Team is undertaking to further advance its mission and vision.

MISSION

The mission of the Privacy Management Team is to facilitate Governor Manchin's vision of implementing the best practices to protect the privacy of personally identifiable information collected, used and disclosed by the Executive Branch.

VISION

The Privacy Management Team recognizes that privacy is a core value of West Virginia citizens and government. The Privacy Program's vision is to ensure:

- *Implementation of best practices and governance to protect personally identifiable information.*
- *Protection of citizens' and employees' personally identifiable information.*
- *Improvement of data quality and protection to enhance West Virginia state government's position in the world market place.*

¹**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.

PRIVACY MANAGEMENT TEAM ACTIVITIES: *A Look Back*

The Privacy Management Team has succeeded in achieving significant accomplishments throughout the past year. The following accomplishments have been completed.

- **Data Assessment:** To obtain a more precise understanding of current Executive Branch department practices regarding how PII is collected, shared, secured, managed and disclosed, the Privacy Management Team researched and built an on-line assessment tool to gather information from each Executive Branch department. The Data Assessment result outcomes will enable the Privacy Management Team and Executive Branch departments to identify current strengths and weaknesses regarding privacy practices. This assessment is a highly useful resource utilized by the Privacy Management Team, enabling the team to advance the adoption of improved privacy practices within the Executive Branch.

- **Privacy Management Team Summit:**

The Privacy Management Team hosted a summit on May 5-6, 2008, at Stonewall Jackson Resort. This summit allowed individuals in attendance to: enhance knowledge of the role of the privacy program, learn how to identify and manage a privacy incident, gain a general understanding of Executive Branch privacy policies, and learn how to better protect PII. The State Privacy Office, in partnership with the Office of Technology, built an incident simulation into the summit agenda providing participants with incident investigation resolution experience through simulated practice.

- **Creation of the WV State Privacy Office Webpage**

(www.wvprivacy.org): The Privacy Management Team guided the redesign and development of the West Virginia State Privacy Office Webpage. This effort encompassed infrastructure requirements and technical issues. The webpage contains a large amount of useful resources and has become an integral tool for accessing privacy related information. The team's continual commitment to privacy principles and intent to make government operations

CITIZENS SUPPORT DATA BREACH NOTIFICATION LEGISLATION

A January 2008 study conducted by AARP showed overwhelming support for West Virginia data breach legislation².

S.B. 340 enables citizens to be notified when a potentially harmful data breach occurs.

²Nelson, B. & Guengerich, T. (2008). *They Want to Know: The Opinions of AARP Members in West Virginia About Data Breach Notification Legislation.*

more transparent will be exhibited through a “Privacy Tip of the Week” issued to all Executive Branch employees. These tips focus on best privacy practices and current issues surrounding privacy.

- **Enterprise-Wide Standardized Privacy Requirements:** West Virginia has been a leader in identifying all privacy-related laws that impact the Executive Branch and utilizing these laws as guidance for the State’s privacy requirements. Specifically, the Privacy Office monitored over 100 applicable federal and state laws and provided an updated summary of all such laws on its Web site. This ensures that all departments have easy reference to the many federal and state laws that regulate the information they rely on to carry out their programs.

- **Privacy Policy Development:** The development of six new privacy policies is a significant accomplishment that exemplifies West Virginia’s commitment to protecting the privacy of PII collected and maintained by Executive Branch departments. West Virginia is one of the first states to issue Executive Branch privacy policies. The policies cover the following areas: Accountability, Consent, Individual Rights, Minimum Necessary and Limited Use, Notice, and Security Safeguards. In the development of the privacy policies, the Privacy Management Team sought and received input from all Executive Branch departments. This input was essential in allowing the Privacy Management Team to develop a threshold for how the Executive Branch protects the privacy of PII. An extensive review of privacy policies has been underway. Privacy policies have been reviewed at the departmental level, cabinet level, Privacy Management Team level and by private sector expert consultation. This extensive review process is necessary to ensure West Virginia privacy policies reflect best practice standards.

- **Privacy Officer Designation:** The Privacy Office collaborated with each Executive Branch department to name a department level Privacy Officer (PO) and establish the Privacy Officer’s roles and responsibilities. Development of the roles and responsibilities offer tangible guidelines and expectations that will guide PO’s in the area of ensuring privacy protection. Furthermore, the roles and responsibilities of the department level PO will assist the

PRIVACY IS GOOD BUSINESS

Ohio recently experienced a data breach due to adhering to an outdated security procedure. The incident is expected to cost the State almost \$3 million³.

Our Privacy Management Team’s vision to implement best practices to protect personally identifiable information will seek to minimize risk in an effort to prevent such breaches, as seen in Ohio, from occurring in the first place.

³Fonseca, B. (2007). *More personal data said to be stolen Ohio government backup tape*. Retrieved from http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=17&articleId=9035723&intsrc=hm_topic.

Privacy Management Team in effectively providing a means of accountability at a department level for privacy related concerns. Ultimately, the designation of a department level PO allowed for the establishment of a privacy infrastructure across the Executive Branch. The establishment of this infrastructure is a major step toward achieving the mission of the Privacy Management Team and is an integral component in the establishment of sound privacy practices throughout the state.

PRIVACY MANAGEMENT TEAM ACTIVITIES: *A Look Forward*

The Privacy Management Team is committed to the development of initiatives which will further enhance our mission and vision. The following initiatives are currently under development.

- **Privacy Policy Implementation:** The issuance of Executive Branch privacy policies will further serve as a catalyst through which the State of West Virginia will continue its commitment in upholding the value of privacy. While departmental compliance with the Executive Branch privacy policies will occur incrementally, the Privacy Management Team recognizes that compliance with the policies will result in better privacy practices.

- **Privacy Training:** In addition to the already established practice of providing weekly privacy tips to Executive Branch employees via e-mail, the Privacy Office is developing privacy awareness Web-based training for 21,000 Executive Branch employees. The privacy awareness training roll-out is planned for 2009. Minimization of breach opportunities due to employee error will be a major focus of the training. Furthermore, a “train the trainer” event targeted at Privacy Officers is planned. This training will provide Privacy Officers with essential tools and guidance to assist them with the implementation of Executive Branch privacy policies.

- **Privacy Program Audits:** The Privacy Management Team will develop a process to audit enterprise-wide privacy programs and will develop measures to remediate certain audit findings. These audits will act as an accountability mechanism, aimed at advancing best privacy practices. Development of this program is planned for 2009.

EMPHASIS ON MINIMIZING BREACH OPPORTUNITIES WILL BE AN INTEGRAL PART OF PRIVACY TRAINING

Providence Health & Services of Seattle has recently paid a \$100,000 settlement following a 2005-2006 breach of privacy in which the information of 386,000 patients was compromised. The Health and Human Services Department reached this resolution with the company after tapes, discs and laptops containing sensitive data were lost or stolen from the home health care company⁴.

Our Privacy Management Team recognizes that employee error is the underlying cause in most breaches and thus focuses its training initiatives to reduce employee error.

⁴Health Imaging News. (2008). *Seattle provider pays HHS \$100K in patient breach settlement*. Retrieved from <http://www.healthimaging.com/content/view/11583/118>

CONCLUSION

As presented in this annual report, the Privacy Management Team has made significant progress in the area of protecting the privacy of personally identifiable information collected and maintained by Executive Branch departments through the accomplishment of many major initiatives. Furthermore, the Privacy Management Team is also focused on undertaking new initiatives which will further advance its mission and vision. In particular, the Privacy Management Team recognizes the crucial role that privacy outreach and training of Executive Branch employees will have upon its goal of protecting the privacy of personally identifiable information. Ultimately, the Privacy Management Team recognizes that privacy itself is not just a legal issue, an audit issue, an information technology issue, a human resources issue, or a policy issue. Privacy, instead, crosses over all of these boundaries. Only through cooperation, communication, and support over all boundary areas, can we begin to move more closely toward reaching our mission and vision concerning privacy protection.

Privacy Principles

- **Accountability:** Assigned roles and responsibilities to assure application of privacy principles to PII.
- **Notice:** Openness regarding the authority for collecting PII; the purpose of the collection; the location of the entity maintaining the PII; with whom the PII may be shared and why; rights an individual has in PII; and the entity's policies, procedures, standards, and practices.
- **Minimum Necessary and Limited Use:** Collection, use and disclosure of PII should be limited to the entity's legal authority and purpose, as set forth in an entity's Notice, including the minimum and necessary PII the entity needs to perform its defined legally permitted task.
- **Consent:** An entity's collection of PII should be contingent upon first obtaining an individual's consent to collection. An entity 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.
- **Individual Rights:** When possible, an entity relies first on the PII it collects directly from the individual. An individual should be afforded the ability to access and copy the PII an entity acquired or maintains, request an amendment of the information an entity maintains and, if such amendment is not undertaken, request that the information be notated. Entities shall provide appropriate means of individual redress which include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.
- **Security Safeguards:** An entity implements the appropriate management, operational and technical controls to preserve the privacy, confidentiality, integrity and availability of PII.

Mission

The goal of the Privacy Management Team is to facilitate Governor Manchin's vision of implementing the best practices to protect personally identifiable information. Additionally, the Privacy Management Team strives to improve data quality and protection to enhance West Virginia State Government's position in the world market place, and build the value privacy brings to West Virginia State Government's trusted branch.

Vision

The Privacy Management Team recognizes that privacy is a core value of West Virginia citizens and government. The Privacy Program's vision is to ensure:

- *Implementation of best practices and governance to protect personally identifiable information.*
- *Protection of citizens' and employees' personally identifiable information.*
- *Improvement of data quality and protection to enhance West Virginia state government's position in the world market place.*



WEST VIRGINIA STATE PRIVACY OFFICE
100 Dee Drive • Charleston, WV 25311

www.wvprivacy.org