2009 State Privacy Office Annual Report

A report by the State Privacy Office
West Virginia Health Care Authority
December 2009

Executive Branch Departments

Governor's Office

Department of Administration

Department of Commerce

Department of Education and the Arts

Department of Environmental Protection

Department of Health and Human Resources

West Virginia Health Care Authority

Department of Military Affairs and 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 ongoing activities concerning the advancement of processes being undertaken to protect the privacy of personally identifiable information (PII) collected and maintained by Executive Branch departments[1]. 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 fulfill the directives of Executive Order 6-06 to facilitate Governor Manchin's vision of implementing the best practices to protect personally identifiable information. The Privacy Management Team strives to improve data protection and quality, and protect the privacy interests of all West Virginians.

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, policies and procedures 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.

[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 made significant accomplishments throughout the 2009 calendar year. The following accomplishments include:

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

  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 website. 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 program.

- **Privacy Policy Implementation:** The State Privacy Office issued six new Privacy Policies approved by the Privacy Management Team on January 30, 2009 with an effective date of August 1, 2009. The time span from issuance to the effective date allowed West Virginia Executive Branch departments to establish a privacy network, and examine internal operations in relation to the policy requirements. Departments worked with their leadership to gain support for processes such as having all

employees sign confidentiality agreements, adding notices on forms, increasing physical and technical safeguards, and training key staff. The State Privacy Office provided support to the departments through hosting a Train the Trainer session, a policy workshop, examples and templates, consultation on forms, and training assistance. Through a well coordinated process, most departments were successful in reaching established benchmarks and completing actions steps. Two factors seemed to directly relate to a departments success, the support of leadership, and the organizational capacity of the department Privacy Officer and their ability to mobilize a privacy network across their department.

A summary of department and agency self- reported implementation outcomes for 9 of 12 organizations within the Executive Branch scope:

- Executive Branch departments have had employees sign Confidentiality Agreements to protect PII, provide Privacy Notices to customers and employees where necessary have instituted new Security Safeguards as a result of the policy implementation, and have a process for ensuring that customers and employees have the ability to correct or amend their personal PII.
- In most organizations Privacy questions or complaints go through the division/agency Privacy Coordinator to the Department Privacy Officer to be addressed.
- Department Response teams meet monthly, quarterly, or as needed.
- Seven departments have examined vendor and contractor agreements for Privacy policy compliance.
- Six departments identified a situation where PII was being collected that was not needed for the task it was being requested for, and took action to stop requesting.
- Seven departments provide choice to customers and/or employees in the processing of their PII.

- **Incident Response Coordination:** The Privacy Management Team crafted a Response to Unauthorized Disclosures procedure for privacy incidents. The procedure gives instructional steps for identifying and responding to an unauthorized disclosure of Personally Identifiable Information that could cause an individual(s) harm, by revealing sensitive information such as health condition, financial account information, or identifiers that could lead to identity theft such as social security number and date of birth. The procedure requires departments to be accountable by providing notice of breached PII to effected individuals. The State Privacy Office assisted with both incidents requiring follow up notice and incidents that were determined to not meet breach criteria. Six departments are using the Response to Unauthorized Disclosures Procedure that was issued by the State Privacy Office. Three departments have developed an internal procedure or alternate process.

- **Statewide Privacy Training Initiative:** The West Virginia Executive Branch encompasses approximately 22,000 state employees. Under the new Accountability Policy, training for all department employees is required. To reach such a large number of employees, and to ensure consistency of message, an online privacy training program is being employed across departments on the Office of Technology Learning Management System. The training can be accessed online, or as a paper based booklet, both versions with a post test and certificate of completion for passing a comprehension assessment. The training is designed to increase awareness of privacy principles and knowledge of new privacy policies. The process of rolling out the training across departments began in November of 2009, and is anticipated to complete in June 2010.

  All Executive Branch departments have or are in the process of training all employees with awareness level, or a more advanced level of training based on Privacy Principals and policies.

- **HITECH –** The President's American Recovery and Reinvestment Act (ARRA) included new privacy requirements under the Health Information Technology for Economic and Clinical Health Act (HITECH) passed on February 13, 2009. HITECH includes 4 parts, one of which is Privacy or Subtitle D. Many of the provisions are effective February 2010 and include: new federal breach notification requirements, regulation of patient health records and vendors, expansion of the business associate provisions, modification of patient /consumer rights under HIPAA, and increased civil penalties. The Privacy Management Team participated in numerous educational sessions to better understand and anticipate the new requirements.

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:

- **Phase II - Privacy Policy Implementation with Boards and Commissions:** A natural next phase for privacy policy implementation is with the over 200 Boards and Commissions that are associated with the Executive Branch. Boards and Commissions will participate in the statewide privacy training initiative; this will increase the level of privacy awareness with this peripheral group. The State Privacy Office and Privacy Management Team will identify appropriate actions for privacy policy alignment given the structure and operations of Executive Branch Boards and Commissions. The State Privacy Office and Privacy Management Team will reach out to the group and work towards privacy inclusion and policy implementation.

- **HIPAA Revisited:** The many changes included in HITECH created the need for a re-assessment of departments' status as a HIPAA covered entity or business associate to a covered entity. This change has greatly increased the number of organizations that are required to comply with the HIPAA Privacy Rule. The State Privacy Office is coordinating a work plan and training schedule to assist PMT members in assessing their status in light of the changes and developing a strategy for compliance. During the course of 2010, Executive Branch Departments will self evaluate and certify their HIPAA classification, participate in a series of six training sessions, develop work plans for compliance, and complete implementation.

Conclusion:

The 2009 calendar year marked a major focus on Privacy, both federal and state. The President's Health Information Technology for Economic and Clinical Health Act created a national privacy and security environment concerned with protections, transparency, and advancement. On the state level, departments initiated an environment of privacy through new policies and procedures, coordinated privacy teams prepared for responses to breached PII, and the "every state worker" participated in a state wide training initiative to increase privacy awareness and their role in protecting Personally Identifiable Information. As 2009 drew to a close, departments reevaluated their HIPAA covered entity and Business Associate status and began gearing up for 2010 HIPAA requirements.