



WEST
VIRGINIA
STATE
PRIVACY
OFFICE

2014
Annual Report



MEMBERSHIP ON THE PRIVACY MANAGEMENT TEAM INCLUDES:

Executive Branch Departments:

- ✚ Governor's Office**
- ✚ Health Care Authority**
- ✚ Bureau of Senior Services**
- ✚ Department of Administration**
- ✚ Department of Commerce**
- ✚ Department of Education and the Arts**
- ✚ Department of Environmental Protection**
- ✚ Department of Health and Human Resources**
- ✚ Department of Military Affairs and Public Safety**
- ✚ Department of Revenue**
- ✚ Department of Transportation**
- ✚ Department of Veterans Assistance**
- ✚ Chapter 30 Licensing Boards**

Representing other Constitutional Officers, Agencies and Higher Education:

- ✚ State Auditor's Office**
- ✚ Department of Agriculture**
- ✚ ERP Board (wvOASIS)**
- ✚ Secretary of State**
- ✚ State Treasurer**
- ✚ West Virginia School of Osteopathic Medicine**

INTRODUCTION

The West Virginia Health Care Authority (HCA) has been directed by the Governor's Office to define and develop an Executive Branch-wide privacy program, maintain the Privacy Management Team (PMT), issue privacy policies, ensure data classification schemes, and conduct privacy audits. The HCA houses the State Privacy Office (SPO) and appointed a Chief Privacy Officer (CPO) to lead the privacy-related activities of the Executive Branch departments under the Governor's auspices.

The PMT has been established to promote the protection of individual's personally identifiable information (PII)¹, while balancing others' right and need to know. The PMT is comprised of Privacy Officers from each Executive Branch department, other Constitutional Officers, Agencies, and Higher Education representatives, as well as other members of state government who lend their expertise to support the team's objectives. The SPO and PMT work together to develop privacy policies and procedures for the Executive Branch departments.

The purpose of this annual report is to depict the PMT's ongoing activities concerning the advancement of processes undertaken to protect the privacy of PII, such as social security numbers, health information, employees' home addresses and driver's license numbers collected and maintained by Executive Branch departments². This report will detail the major

¹**Personally Identifiable Information (PII):** All information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information (PHI). PII is contained in public and non-public records. Examples may include but are not limited to a specific individual's: first name (or initial) and last name (current or former); geographical address; electronic address (including an e-mail address); personal cellular phone number; telephone number or fax number dedicated to contacting the individual at his or her physical place of residence; social security account number; credit and debit card numbers; financial records, including checking, savings and other financial account numbers, and loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints, palm prints, facial recognition, full face image and iris scans; driver identification number; birth date; birth, adoption or death certificate numbers; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet Cookie; and criminal records and history. When connected with one or more of the items of information specified above, PII includes any other information concerning an individual that, if disclosed, identifies or can be used to identify a specific individual physically or electronically.

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

accomplishments of the PMT, as well as address new initiatives the PMT is undertaking to further advance its mission and vision.

Mission

The mission of the PMT is to facilitate West Virginia's vision of implementing best practices and legal requirements to protect PII. The PMT strives to improve data protection and quality and protect the privacy interests of all West Virginians.

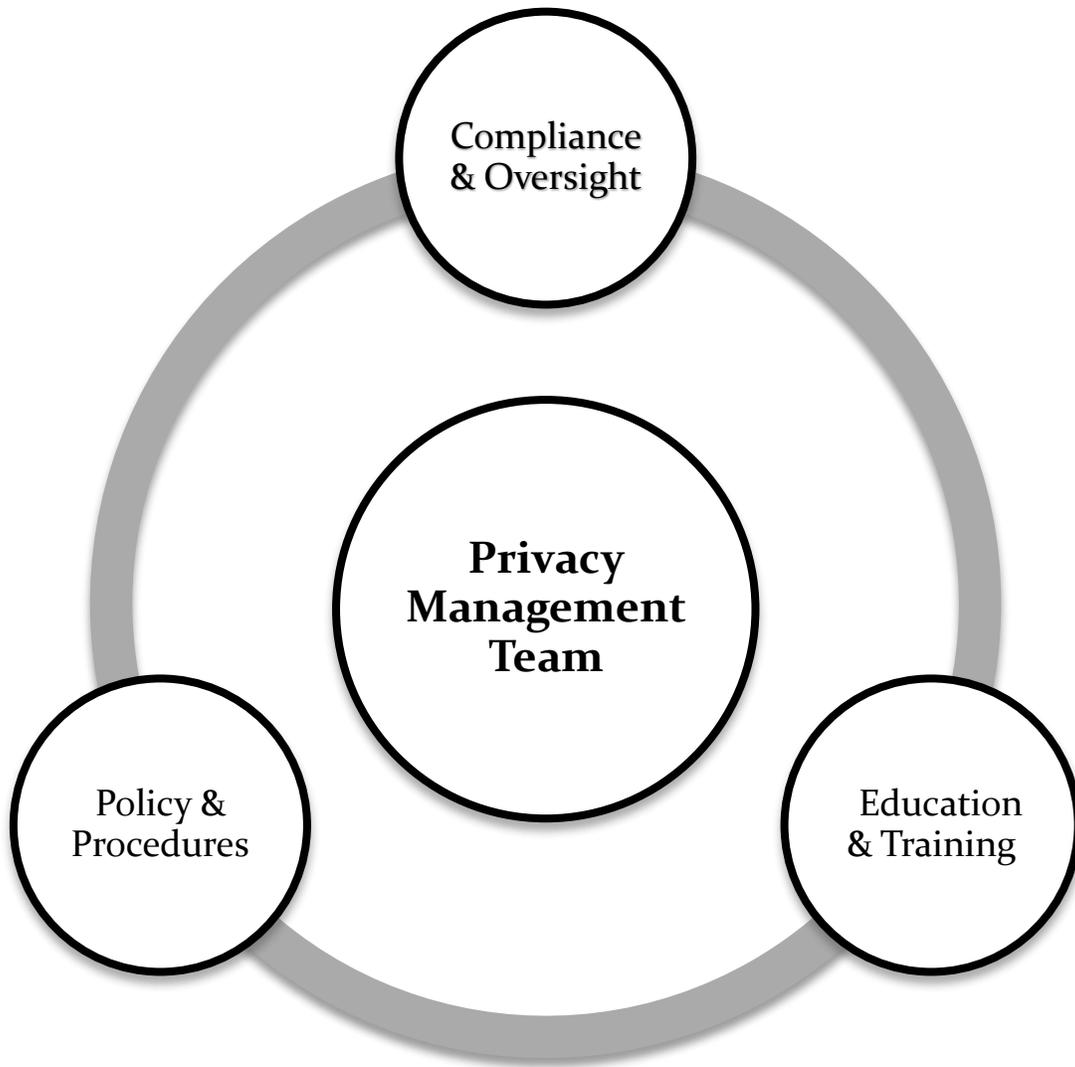
Vision

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

- Implementation of laws, regulations, best practices, policies and procedures to protect PII;
- Protection of citizens' and employees' PII; and
- Improvement of data quality and protection to enhance West Virginia State Government.

PMT: 2014 OBJECTIVES

In 2014, the PMT strived to meet its mission and vision by focusing on the following key privacy program objectives:





COMPLIANCE & OVERSIGHT

To accomplish its mission, the PMT assures that each department complies with privacy policy and procedures to protect PII. The SPO provides consultation and research to support the PMT and departments as they integrate measures to ensure improvement of data quality and the protection of citizens' and employees' PII.

Confidentiality Agreement

Along with privacy training, one of the biggest weapons in the arsenal against insider threats is execution of a strong confidentiality agreement. The West Virginia Executive Branch Confidentiality Agreement sets forth the terms and conditions required of every member of the workforce with respect to confidential data. These terms and conditions are effective throughout the lifetime of the worker. In 2014, Confidentiality Agreement enrollment was completed on the State's Learning Management System (LMS) resulting in at least 81 percent completion³ by all Executive Branch departments.

Consultation & Research

The SPO provided the Department Privacy Officers (DPO) and departments the following consultation and research services in 2014:

- Provided privacy legal advice and consultation regarding privacy policies, procedures, laws, regulations, best practices, implementation, and privacy in project design.
- The SPO along with PMT members continued to support the wvOASIS project. wvOASIS (Our Advanced Solution with Integrated System) is an Enterprise Resource Planning (ERP) system which comprises a suite of commercially-available integrated modules that allows an organization to use a system of integrated applications to manage its business functions. Representatives from the wvOASIS project attended PMT meetings in 2014 and provided status reports related to the PII identification and requirement process. From time to time,

³ The percentage does not reflect inactive employees, employees who manually take the training or contractors/vendors.

the SPO provided wvOASIS with technical assistance. For example, wvOASIS asked the PMT for a decision on a privacy issue impacting accounts payable across the State that was legally sound, that could be relied upon in the face of challenge, and that would have buy-in from all wvOASIS impacted organizations. The SPO constituted a workgroup from a cross-section of the PMT, including Privacy Officers from departments within the Governor's Cabinet, as well as Privacy Officers from other constitutional officers, to create a solution. The workgroup's recommendation was presented to the PMT at its October 2014 meeting for its approval which the SPO delivered to wvOASIS.

- The SPO and PMT worked with the Executive Director of the West Virginia Board of Risk & Insurance Management (BRIM) to obtain cyber insurance coverage for the West Virginia Executive Branch departments.
- The SPO provided consultation related to privacy policies, program design and incident response plans for several non-Executive Branch agencies which included the Department of Education, the Treasurer's Office and the Auditor's Office. The Treasurer's Office along with the Auditor's Office is represented on the PMT.

Incident Response

In order to ensure adherence with state privacy policy, as well as federal and state privacy laws, the SPO continued to provide incident response support to all Executive Branch DPOs. The SPO served as a resource, offering guidance and advice throughout the incident process, from the initial report, throughout the investigation, until the privacy incident was resolved.

Privacy Self-Assessment

In late 2010, the SPO and the PMT formed a partnership with BRIM. BRIM provides casualty insurance coverage for all state agencies, including protection against lawsuits and other liability claims resulting from privacy related incidents. BRIM agreed to support the PMT through financial incentives to agencies within the Executive Branch, as well as agencies outside the Executive Branch to complete privacy self-assessments and this support has continued to date. A privacy self-assessment is a tool designed to help privacy professionals assess their privacy programs. Executive Order No. 6-06 empowers the HCA to conduct audits of privacy programs.

The PMT selected the *Generally Accepted Privacy Principles* (GAPP) as the audit framework⁴ as it is based upon fair information practices and contains criteria of good privacy practices found in privacy laws and regulations, both nationally and internationally.

The 2014 self-assessment asked departments to certify: a) all employees on board as of May 31, 2014 have signed West Virginia Executive Branch Confidentiality Agreements, b) all existing employees on board as of May 31, 2014 had received privacy training, c) all laptops with PII, including protected health information (PHI), had been encrypted, d) all unauthorized disclosures are reported in compliance with the Response to Unauthorized Disclosures Procedure, and e) the self-assessment for the following principles had been completed; Management, Notice, Choice and Consent, Collection, Access, Disclosure to Third Parties, Security for Privacy, Quality, Monitoring and Enforcement, and Use, Retention and Disposal. Roll-out for the 2014 privacy self-assessment began July 1 with a completion date of November 17, 2014 for the survey. The self-assessments were completed by DPOs and Agency Privacy Officers, then reviewed and certified by their respective Cabinet Secretaries. The self-assessments and certifications were submitted to the SPO by November 21, 2014, with a certification rate of 83 percent by Executive Branch agencies, excluding the Chapter 30 Licensing Boards.

PRIVACY IMPACT ASSESSMENT (PIA)

A PIA is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed implementation of a system. PIAs are considered a key component of privacy programs. All organizations need to implement processes to identify projects that impact privacy and build in key controls during the earliest stages of those initiatives. In 2014, the SPO completed its research on best practices and along with the PMT formed a workgroup to ensure the West Virginia Executive Branch has a PIA process in place. The workgroup completed a PIA guidance document and developed questions for a web-based PIA form. HCA Information Technology staff began work on the ePIA form with a December 2014 completion date. Training on the new PIA process will be scheduled in early 2015.

⁴ The audit framework (GAPP) is designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities. The primary objective is to facilitate privacy compliance and effective privacy management. The secondary objective is to provide suitable criteria against which a privacy attestation engagement (usually referred to as a privacy audit) can be performed.



EDUCATION & TRAINING

Data Privacy Day

For the fourth consecutive year, the West Virginia Executive Branch championed *Data Privacy Day*, January 28, 2014 as a day to highlight the importance of the protection of personal and private data, and remind us to remain vigilant and proactive about protecting the information that others have entrusted to us. The genesis of *Data Privacy Day*, in the United States and Canada, was in January 2008 and was an extension of the *Data Protection Day* celebration in Europe. The United States Senate issued a resolution, sponsored by Senator John D. Rockefeller IV, recognizing January 28th as *National Data Privacy Day* for the fourth year in a row.

In furtherance of the support of *Data Privacy Day*, Governor Earl Ray Tomblin issued a Proclamation declaring January 28, 2014 as *Data Privacy Day* in West Virginia. The Proclamation recognized Executive Order No. 6-06, giving the Chair of the HCA the responsibility for protecting the privacy of PII collected and maintained by Executive Branch agencies. The HCA leads and staffs the team and houses the SPO for the Executive Branch. The Governor's Proclamation is a yearly reminder that we all share the responsibility to be conscientious stewards of data by respecting privacy, safeguarding data and enabling trust. *Data Privacy Day* is an effort to empower and educate people to protect their privacy, control their digital footprint, and make the protection of privacy and data a great priority in their lives.

PMT Professional Development

The SPO hosted the following webinars for PMT members:

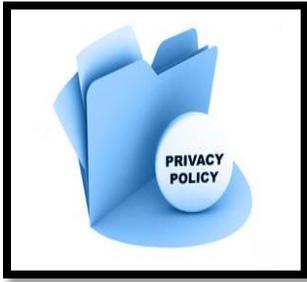
- 2014 Updates to West Virginia Executive Branch Privacy Requirements and HIPAA Preemption Analysis
- *Confronting HIPAA & HITECH Vulnerabilities in Health Data Registries*
- *OCR HIPAA Audits ... Will You Be Prepared?*

Workforce Development

The SPO and PMT continued under the three-year (2012-2015) training plan, ensuring that employees receive appropriate training and education regarding privacy laws, regulations, policies, standards, and procedures governing the handling of PII. In 2014, the PMTs focus was on privacy awareness. Additionally, departments continued to deliver privacy policy training to their workforces.

Privacy Awareness

- *Privacy Rocks!* This training is offered through the West Virginia State Learning Management System (LMS). The training provides an overview of what is privacy, how to handle personal information, privacy responsibility and privacy policies.
- Who is required to take this training? All Executive Branch Workforce
- In 2014, *Privacy Rocks!* enrollment was completed, resulting in 81 percent completion by all Executive Branch departments. (Percentage does not reflect inactive employees and/or employees who manually take the training, or contractor/vendors.
- 26 Privacy Tips, covering all aspects of privacy, were delivered to the workforce.



POLICY & PROCEDURES

Privacy Requirements

Each department must operate within its legal authority and restrictions with regard to the collection, use, disclosure and retention of PII. The Privacy Requirements document reviews laws that impact the enterprise. Necessarily, there will be privacy laws not covered in the report, as they impact isolated agencies. This report is updated on an annual basis, with issuance in the fall of each year. Laws are divided into two categories, Federal and State. Each law is identified by its common name, legal citation with a description, implications and electronic source. The 2014 update to the West Virginia Executive Branch Privacy Requirements includes all relevant privacy legislative and congressional enactments, regulations, and court decisions since June 2013. This online resource is used by privacy professionals and communicated to the West Virginia State Bar.

Revised Response to Unauthorized Disclosures Procedure

The *Response to Unauthorized Disclosures* procedure was revised and finalized for distribution in September 2014. This procedure was revised in response to the new cyber insurance requirements.

HIPAA/HITECH⁵

- With the HIPAA Preemption Chair, the SPO updated the HIPAA preemption analysis and amended policies to ensure application of more stringent West Virginia law passed in 2014.
- The HIPAA Preemption Chair researched and further analyzed several issues related to the new rules under HIPAA. Resolution of these issues resulted in revisions made to the HIPAA/HITECH policy templates.

⁵ Health Information Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH Act).



LOOKING AHEAD TO 2015

Compliance & Oversight

- **Consultation & Research:** The SPO will continue to provide DPOs and departments with on-going support with their privacy questions and privacy related consultation and research.
- **Privacy Self-Assessment:** In an ongoing commitment to protect privacy and reduce liability, the SPO will convene a workgroup to evaluate the 2014 privacy self-assessment and determine the 2015 program.
- **wvOASIS:** The SPO will continue to coordinate with wvOASIS to facilitate privacy implementation for the project and will provide advice and consultation as requested. Additionally, the SPO will serve as a liaison between the wvOASIS project team and the DPOs to ensure privacy objectives are met in a way that is beneficial to the project. Finally, the CPO will chair the wvOASIS Combined Breach Incident Response Team, which will develop, document and educate stakeholders on appropriate incident response, as well as serve as a consulting resource to the wvOASIS Steering Committee.

Education & Training

- As an ongoing demonstration of support for privacy efforts in West Virginia, the SPO anticipates that Governor Earl Ray Tomblin will once again issue a Proclamation declaring January 28, 2015 as Data Privacy Day in West Virginia. The theme for Data Privacy Day 2015 will be: “Respecting Privacy, Safeguarding Data and Enabling Trust.” To celebrate this day, the SPO will orchestrate a variety of privacy awareness events, tips and activities for the West Virginia Executive Branch workforce, to highlight the importance of protecting PII.
- The SPO will continue to support each DPO with their overall privacy training program which will include privacy awareness training for new workforce members, on-going

professional development of DPOs and privacy awareness tips for West Virginia Executive Branch workforce members. In 2015, the SPO will revamp the Privacy Awareness training module to ensure the content is fresh, include updated Privacy information and ensure workforce learning engagement with the new training.

Policy & Procedures

- The SPO and PMT will revise the West Virginia Executive Branch Privacy Requirements for any relevant updates based upon privacy legislative and congressional enactments, regulations, and court decisions.
- The SPO and HIPAA Preemption Chair will update the HIPAA Preemption Analysis and revise policy as needed.

CONCLUSION

As stated in the introduction section of this report, the overall mission of the PMT is to ensure facilitation of the West Virginia privacy program strategic goals and objectives. This encompasses implementing best practices such as the PIA and ensuring legal requirements are kept updated to protect PII. In 2014, West Virginia Executive Branch departments raised the bar for ensuring integrity with their privacy self-assessments and accountability with their privacy awareness training and confidentiality agreement compliance within the West Virginia Executive Branch workforce. Again in 2014, it was a great honor to have Governor Earl Ray Tomblin sign a Proclamation designating January 28 as *Data Privacy Day* in West Virginia.

The SPO provided privacy policy leadership and expertise to several non-Executive Branch agencies. By advancing West Virginia Executive Branch privacy program best practices to non-Executive Branch agencies, the PMT not only gains additional partnerships, outreach efforts enhance public trust because state government is committed to data protection practices.

It is anticipated that 2015 will be a year replete with a new privacy awareness training course, a Privacy Retreat for PMT members to ensure professional development opportunities, HIPAA auditing preparation, a new process that will ensure privacy is embedded in new systems and updated programs. Most importantly the PMT will strive to ensure an ongoing commitment to protecting the PII entrusted to the Executive Branch of West Virginia state government.