West Virginia State Privacy Office

2012 Annual Report

A Report by the State Privacy Office
West Virginia Health Care Authority
December 2012

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 Boards

Introduction

The purpose of this annual report is to depict the Privacy Management Team's (PMT) ongoing activities concerning the advancement of processes being undertaken to protect the privacy of personally identifiable information (PII)[1], such as social security numbers, employees' home addresses and driver's license numbers collected and maintained by Executive Branch departments[2]. The report will detail the major 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.

[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.

Privacy Management Team: A Look Back at 2012

The PMT made great strides in privacy protection during the 2012 calendar year, including the following:

Data Privacy Day

For the third consecutive year, the West Virginia Executive Branch championed *Data Privacy Day*, January 28, 2012, 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 28, 2012 as *National Data Privacy Day* for the fourth year in a row.

Governor Earl Ray Tomblin's Privacy Proclamation

In furtherance of the support of Data Privacy Day, Governor Earl Ray Tomblin issued a Proclamation declaring January 28, 2012 as Data Privacy Day in West Virginia. The Proclamation, signed on January 16, 2012, recognized Executive Order No. 6-06, giving the Chair of the West Virginia Health Care Authority (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 State Privacy Office (SPO) for the Executive Branch.

Privacy After Hours

The International Association of Privacy Professionals (IAPP) approved the SPO to host a *Privacy After Hours* event held on February 2, 2012. Privacy After Hours provided a wonderful opportunity to meet other privacy professionals from the area, network, and engage in lively discussion in a relaxing environment.

PMT 2012 – 2015 Training Plan

The SPO and PMT embarked on a project to develop a three-year training plan to ensure that employees receive appropriate training and education regarding privacy laws, regulations, policies, standards, and procedures governing the handling of PII. The training plan outlined the responsibilities of the SPO, Department Privacy Officers (DPOs), Privacy Coordinators and members of the workforce.

Privacy Awareness Training

One of the most exciting accomplishments of 2012 was the development of *Privacy Rocks!,* a new privacy awareness training course. *Privacy Rocks!* is certain to help build privacy awareness by using a stimulating, creative approach that will challenge the learner. Real-life scenarios, case studies, knowledge checks, West Virginia scenery and artwork were provided to add relevance and increase comprehension and retention. *Privacy Rocks!* will enable employees to identify and understand what PII is, how to manage it, and make informed decisions regarding protection.

All employees will be required to enroll in *Privacy Rocks!*, via the West Virginia Office of Technology's (WVOT) Learning Management System (LMS) or in an alternative format, ultimately reducing risk of a privacy breach for West Virginia Executive Branch departments. Good data protection practices will strengthen citizen trust in state government – an essential element in maintaining credibility.

HIPAA Refresher and HITECH Implementation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has new privacy requirements under the Health Information Technology for Economic and Clinical Health Act (HITECH Act) passed on February 13, 2009. To ready the workforce for these new changes, a "HIPAA refresher" online training course was deployed, which was required training for all covered entities and internal business associates (BAs)[3] within the Executive Branch. The refresher course was offered through the LMS and remains available for new employees and BAs.

[3] **Business Associate**: A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and re-pricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

In 2012, the *West Virginia State Government HIPAA Business Associate Addendum* (BAA)[4], was recognized as an exemplar in a report issued by the Office of the National Coordinator for Health Information Technology, in partnership with the Substance Abuse and Mental Health Services Administration. Charlene Vaughan, PMT member, Vendor/Business Associate Subcommittee Chair and Deputy Attorney General for the Department of Health and Human Resources, led the development of the WV BAA, which is incorporated by reference in all State contracts issued by the Purchasing Division.

Confidentiality Agreement

The Ponemon Institute recently released a report advising that the cost of a data breach was $194 per lost record, highlighting the importance of employee awareness and adherence to policies that protect PII. The report stated that "[t]hirty-nine percent of organizations say that negligence was the root cause of the data breaches. Accordingly, organizations need to focus on processes, policies and technologies that address threats from the malicious insider or hacker." (Ponemon Institute LLC, *2011 Cost of Data Breach Study - United States*, March 2012, pp.2-3). 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 2011, the PMT took the unprecedented step of creating one uniform confidentiality agreement for all Executive Branch employees, and establishing an electronic process such that it would "follow" them as they transfer within the Executive Branch.

The PMT began deployment of this agreement through the WVOT LMS in 2012. Five departments have been enrolled in the Confidentiality Agreement, with seven remaining. All Executive Branch departments are anticipated to complete the agreement by April 30, 2013.

Privacy Self-Assessment

In late 2010, a partnership was formed between the HCA and the West Virginia Board of Risk and Insurance Management (BRIM). BRIM provides casualty insurance coverage for all state agencies, including protection against lawsuits and other liability claims resulting from incidents. BRIM agreed to support the PMT through financial

[4] **Business Associate Addendum**: An addendum to a purchasing contract between a covered entity and its vendors who will use protected health information (PHI) for administrative, research, pricing, billing or quality-assurance purposes. Business Associates are not only providers of health care services; they might be individuals or entities involved in legal, accounting or financial services.

incentives to agencies within the Executive Branch to complete privacy self-assessments and this support has continued to date. The 2012 self-assessment asked departments to certify as to the number of employees with access to PII and that they had met the following four criteria: (1) all privacy policies had been implemented, (2) all existing employees on board as of May 31, 2012 had received privacy training, (3) all laptops with PII, including protected health information[5], had been encrypted, and (4) the self-assessment for the following principles had been completed: Management, Notice, Choice & Consent, Collection, Disclosure to Third Parties and Access.

The *Generally Accepted Privacy Principles* (GAPP) was selected as the audit framework 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 self-assessments were completed by DPOs and Agency Privacy Officers, then reviewed and certified by their department Cabinet Secretaries. The self-assessments and certifications were submitted to the SPO by October 31, 2012, with a completion rate of 93% by Executive Branch agencies, excluding the boards and commissions.

The SPO and BRIM together determined that in addition to the financial incentive for completion of the privacy self-assessment, a recognition component would be introduced in 2012. Every DPO who had 100% of his or her agencies complete the self-assessment and the appropriate Cabinet Secretary certified to the same, was invited to attend a photo opportunity with Governor Earl Ray Tomblin and received a certification of recognition from the Governor.

State Privacy Office's Support of the PMT

The SPO served all West Virginia State Government departments within the Executive Branch, in a multiplicity of ways:

Privacy Compliance

In addition to answering every question we received from every department, the SPO continued to serve in the following capacities in 2012:

[5] **Protected Health Information (or PHI)**: A subset of PII and means**,** with regard to HIPAA covered entities (*see* 45 C.F.R. §106.103), individually identifiable health information, including demographic information, whether oral or recorded in any form or medium that relates to an individual's health, health care services and supplies, or payment for services or supplies, and which identifies the individual or could reasonably be used to identify the individual.

- Provided privacy legal advice and consultation regarding privacy policies, procedures, laws, regulations, best practices, implementation, and privacy in project design.
- Gave presentations and served as subject matter experts to various state government audiences regarding current privacy topics and trends.
- Offered to the PMT to review department and agency privacy notices and audit them against the Notice Policy. Several agencies took the SPO up on this offer and the SPO provided them with feedback and suggestions.
- The West Virginia Executive Branch receives copious West Virginia Freedom of Information Act (FOIA) requests. The SPO supported DPOs and others in reviewing proposed disclosures to ensure PII was appropriately and legally redacted. The SPO coordinated with the Attorney General's Office on this matter.
- Worked to ensure that there is a Privacy Officer in every department and follow up with the Governor's Office as necessary.
- Made sure that each DPO understood their role and responsibilities, received new privacy officer orientation and training and that they were given any assistance needed.
- Provided advice and consultation regarding proposed statutory or legislative changes.

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 Website Redesign

The SPO's website (www.privacy.wv.gov) was given a fresh, new look and has been updated and reorganized. New pages have been created (Legal & HIPAA) and others have been organized in a more user-friendly order. As the SPO's primary function is to support privacy compliance in the Executive Branch, the website is geared toward helping the workforce find information on privacy policies, procedures and resources. There are links to privacy documents, department-specific privacy laws and rules, as well as links to external websites that may be beneficial to privacy officers and other state employees. The SPO added a page for consumers, providing useful information and links related to HIPAA and other entities for which they may need. New graphical design options are under consideration and should be applied early in 2013.

Automated PII Search

Tom Petersen, Database Administrator in the Information Technology Division of the HCA, developed a program to search documents for PII. As a whole, state government receives many documents from the public and some contain inappropriate PII. At the request of the Chief Privacy Officer, Tom provided a demonstration of the program with the team members during the June PMT meeting. Many of the PMT members were interested in pursuing the tool for use with their departments and were invited to follow up with the SPO for assistance.

HIPAA Business Associate Workshops

The HITECH Act makes BAs directly subject to parts of HIPAA. As part of the HITECH Act, BAs are made subject to civil and criminal enforcement actions. In order to assist departments impacted by the HITECH Act, the SPO provided six workshops, as well as policy templates, to the West Virginia Executive Branch BAs to facilitate their compliance with the HIPAA Privacy Rule.
The workshops covered the following topics:

- Use, disclosure, minimum necessary
- Workforce policies
- Patient's rights
- Incident response
- Document retention
- Safeguards

Preemption Analysis/Bar Blast

Because HIPAA does not preempt state law, it is essential to maintain a current and accurate preemption analysis to determine whether state law imposes additional privacy requirements on departments upon the HIPAA floor. State laws that are contrary to the Privacy Rule are preempted or voided by the Federal requirements, unless a specific exception applies. (See 45 C.F.R. Part 160, Subpart B.)

The preemption analysis chart is updated on an annual basis and provides an overview of West Virginia's health-related laws and an analysis of the preemption issues. The 2012 update includes all relevant West Virginia legislative enactments since June 2011, and is reflective of the HITECH Act and regulations. In addition to the preemption analysis itself, a summary document including background information, FAQs and a flow chart were included to facilitate understanding of this complex topic.

The preemption analysis is also a useful resource to health care providers and practicing attorneys outside state government. The SPO partnered with the West Virginia State Bar in making this preemption analysis available to West Virginia lawyers by its publishing its URL in the November 2012 Bar Blast that is distributed to its membership.

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 2012 update to the West Virginia Executive Branch Privacy Requirements includes all relevant privacy legislative and congressional enactments, regulations, and court decisions since June 2011.

Support for Statewide Initiatives

The SPO, with the PMT, offered support in the realm of privacy for a variety of West Virginia statewide initiatives:

wvOASIS Project

The wvOASIS team provided the PMT with a project overview at the October 2012 meeting. The overview included a description of the project goals, its scope, phases and opportunities for agency input. wvOASIS will utilize a number of different personal identifiers to track employees and citizens across its database. The PMT was very interested in learning more about the project, particularly with respect to the inclusion of PII from the departments.

Many DPOs offered questions and concerns about the safeguards to be applied to personal information maintained by their respective departments. wvOASIS was asked to implement privacy controls to safeguard West Virginia Executive Branch PII. wvOASIS responded that it was open to better understanding the privacy controls being recommended, and they requested a list of enterprise-wide data elements that require privacy protection, along with the proposed controls.

To assist wvOASIS, the PMT identified those data elements that are processed across the enterprise and require privacy protection. The PMT utilized the West Virginia FOIA as a framework to identify the data elements and information requiring special handling.

Given that wvOASIS is a project of the Governor, the Auditor and the Treasurer, the PMT determined that recommendation of a national set of controls would be the most appropriate response. The PMT has significant experience with the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants' GAPP and recommended to wvOASIS that it adopt GAPP as its framework to build privacy into the project design. This framework has emerged as a premier privacy framework in use today and is implemented in both the private and public sectors for purposes of developing a privacy program, as well as an audit tool.

The SPO submitted a memorandum regarding the above, along with its recommendations to wvOASIS in December 2012 and looks forward to supporting and coordinating with this project.

Document Retention

At the April PMT meeting, Donna Lipscomb, Executive Coordinator / Legislative Liaison for the Department of Administration provided members with an overview of the state plan for document retention. Because of the significant intersection between document retention and privacy, the PMT is very much interested in supporting the statewide initiative in the development of a state plan. Ms. Lipscomb agreed to keep the SPO and PMT apprised of developments in the document retention plan, and to let the team know how it could help.

International Public Management Association for Human Resources (IPMA-HR)/Bring Your Own Device (BYOD):

In April 2012, the IPMA-HR West Virginia Chapter requested the SPO to participate in a panel presentation exploring the human resources implications of BYOD. The IPMA-HR is an organization "representing the interests of human resource professionals at the federal, state and local levels of government." The SPO provided information and guidance regarding privacy implications, such as using personal phones, laptops, iPads, iPods, and computers with personal, non-state data on them. In light of the growing trend toward using personal devices in the workplace, the SPO provided training for the PMT on BYOD at the June meeting.

Realizing that BYOD will continue to be an area of concern and challenge for West Virginia Executive Branch departments, the SPO will stay abreast of developments and serve as a privacy resource as requested.

REAL ID Act

Natalie Harvey, Public Information Director for the Division of Motor Vehicles (DMV), offered a presentation at the February PMT meeting on the new secure driver's license and ID card requirements that were prompted by the REAL ID ACT of 2005. The REAL ID Act came about as an anti-terrorism measure and established a rule to create federal standards for driver's licenses. Attendees at the February PMT meeting were able to learn about the new law's privacy and security requirements, including data collection, use and storage, and what to expect as the DMV moves forward with meeting the Federal requirements. Jill Dunn, General Counsel for the DMV, provided additional information and clarification at the May PMT meeting.

GEIST/Workplace Assessment

The PMT works in collaboration with the Governor's Executive Branch Information Security Team (GEIST) to ensure the privacy and security of information within and across departments, in conformance with privacy and security laws and policies. The Chief Privacy Officer, and the WVOT's Chief Information Security Officer, in a discussion about audit obligations of the WVOT and the achievement of improved levels of security and privacy practices throughout the State, agreed on the value of implementing a workplace self-assessment program. The WVOT agreed to lead and manage this project.

The goal of the workplace self-assessment is to validate that sensitive information is properly managed in both paper and electronic forms, throughout state government offices, by performing validation checks on a regular schedule. The assessments look for sensitive documents left unattended on printers, fax and copy machines, as well as on desktops and other locations. In addition, workstation areas are checked for viewable passwords, unattended workstations, publicly viewable monitors that might display confidential information, and the proper management of the public in secured building areas. The results of the assessments are entered into an online, web-hosted database for reporting back to departmental leadership, and the Privacy and Security offices. The program was launched in October, 2012.

Privacy Management Team Activities: A Look Forward

Data Privacy Day 2013

As an ongoing demonstration of support for privacy efforts in West Virginia, we anticipate Governor Earl Ray Tomblin will issue a Proclamation declaring January 28, 2013 as Data Privacy Day in West Virginia. The theme for Data Privacy Day 2013 is "respecting privacy, safeguarding data and enabling trust" with a goal of participation by individuals, companies, organizations and government agencies. To celebrate this day, the SPO will orchestrate a variety of privacy awareness events and activities for the West Virginia workforce, to highlight the importance of protecting personally identifiable information.

Privacy After Hours

Once again, the IAPP has selected the SPO as the Charleston host for a Privacy After Hours event to be held on January 23, 2013. This should be another exciting opportunity to network with privacy professionals from state government, as well as the private sector.

Confidentiality Agreement Execution

The PMT will continue the deployment of the *West Virginia Executive Branch Confidentiality Agreement* through the WVOT LMS in 2013, with a goal of all Executive Branch departments having completed execution of the agreement by April 30, 2013.

Privacy Awareness Training

As noted earlier, the SPO and PMT are very excited about the development and deployment of the new privacy awareness training course, *Privacy Rocks!.* The enrollment began in December 2012 and the goal is for each Executive Branch department to have a completion rate of 85% by June 20, 2013. The training demonstrates state government's commitment to data stewardship, safeguarding PII and reducing the risk of privacy breaches in West Virginia Executive Branch departments. As a result of risk reduction, citizen trust is strengthened and credibility in state government is elevated.

Privacy Self-Assessment

In an ongoing commitment to protect privacy and reduce liability, the HCA and BRIM will continue to partner by convening a workgroup to evaluate the 2012 privacy self-assessment and shape the 2013 assessment. The following principles will be added to the assessment:

- Use, retention, and disposal
- Security for privacy
- Quality
- Monitoring and enforcement

It is anticipated that BRIM will continue to provide a financial incentive component and hope to continue with the recognition component by Governor Earl Ray Tomblin. The SPO and BRIM will evaluate additional program elements to motivate participation in this program.

HITECH Implementation

The final HITECH Act regulations are now expected in 2013, which will dictate the need for policy development and revision of the West Virginia BAA. Once the regulations are finalized, policy training and implementation will take place with the PMT, with workforce training occurring thereafter.

Privacy Workshop

An educational event is planned for the PMT in October, 2013. The purpose of this event is to provide training and education regarding privacy laws, regulations, policies, standards, and procedures governing the Executive Branch's handling of PII. A workgroup, comprised of PMT members, will be formed to create the agenda. It is anticipated that much of the workshop will focus on current challenges such as BYOD, social media, portable device management, such as smart phones, incident response and investigations. Plans also include providing learning opportunities for individual development around change management, team building and managing from the middle.

Coordination with wvOASIS

The SPO will follow up 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 DPOs to ensure privacy objectives are met in a way that is beneficial to the project.

Conclusion

In 2012, a renewed emphasis on privacy was realized by Executive Branch DPOs and agency level Privacy Coordinators, in turn capturing the attention of the West Virginia workforce. It was a great honor to have Governor Earl Ray Tomblin sign a Proclamation designating January 28 as Data Privacy Day in West Virginia. From the numerous requests for additional training, the feedback on privacy tips, and the participation in privacy-related events, it is obvious that privacy is advancing as a priority in the planning and design phases of major projects in state government.

With a robust commitment by the SPO and PMT to prioritize privacy and data protection practices in 2013, citizen trust will be increased and credibility will be elevated. It is anticipated that 2013 will be a year replete with new and exciting privacy training, educational opportunities, and an ongoing commitment to protecting the PII entrusted to the Executive Branch of West Virginia State Government.