West Virginia State Privacy Office

2011 Annual Report

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

Executive Branch Departments

- Governor's Office
- WV 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 Privacy Program's vision is to ensure:

[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.

- 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.

Privacy Management Team: A Look Back, 2005 - 2010

The Journey Begins

Since its inception in September 2005, the Executive Branch-wide Privacy Management Team (PMT) has worked to promote the protection of personally identifiable information (including PHI) while balancing others' need and right to know. The PMT works in collaboration with the Governor's Executive Branch Information Security Team (GEIST) to realize the benefits of information flows within and across Departments, in conformance with privacy policies and laws. All Executive Branch departments have Privacy Officers participating on the PMT.

On August 16, 2006, Governor Joe Manchin III signed Executive Order No. 6-06 giving the Chair of the West Virginia Health Care Authority (HCA) the responsibility for protecting the privacy of personally identifiable information collected and maintained by Executive Branch agencies. The West Virginia Health Care Authority leads and staffs the team and houses the State Privacy Office for the Executive Branch. On January 16, 2012, Governor Earl Ray Tomblin issued a Proclamation recognizing this Executive Order and declaring January 28, 2012 as Data Privacy Day in West Virginia.

The State Privacy Office serves all West Virginia State Government Departments within the Executive Branch by:

- Facilitating development and then issuance of Executive Branch-wide Privacy Principles, Privacy Policies, and Privacy Procedures;

- Developing and annually updating the WV Executive Branch Privacy Requirements, which is a survey of all privacy laws impacting the enterprise;
- Developing and annually updating the HIPAA Preemption Analysis;
- Answering privacy questions from every Department;
- Working to ensure that every Department has a privacy officer;
- Making sure that the privacy officer understands his/her role and responsibilities;
- Providing training;
- Leading and facilitating Departments' privacy self-assessments; and
- Providing assistance and support as needed.

Discovery

In order to develop a privacy program, the PMT embarked on a mission to determine what the goals of the program would be and how to achieve those goals while adhering to state and federal laws. Each Department Privacy Officer examined the information practices within his or her department, and identified issues that needed to be addressed. Best practices and laws were reviewed and the following privacy policies were drafted by the HCA, with input from the PMT and issued by the HCA Chair:

- Accountability;
- Notice;
- Consent;
- Individual Rights;
- Minimum Necessary and Limited Use; and
- Security Safeguards.

Building

Once the groundwork was laid, the PMT set out to develop procedures to support the policies. The procedures had to meet the goals set forth by the policy and be achievable by the workforce charged with following and adhering to them. The PMT worked extremely diligently to implement the privacy policies and procedures.

Communicating

Policy was written and in place; procedures were written and in place; it was time to train the workforce. Privacy awareness training was developed and deployed online, via the Office of Technology's Learning Management System (LMS). All Executive Branch employees were required to take the training, entitled *Privacy Basics*, and this training remains a requirement for new members of the workforce.

The PMT felt it was important to provide ongoing training to the workforce. It was determined that weekly privacy tips would be a good mechanism to provide this training. The State Privacy Office began preparing privacy tips, tied to privacy policy, and sending them to the Department Privacy Officers for dissemination to their employees.

Evolving

From the beginning, the PMT recognized that building and maintaining a privacy program would be an ongoing, evolving process, requiring both vigilance and flexibility. In order to ensure ongoing compliance with Executive Branch Privacy Policies and Procedures, as well as state and federal law, the PMT has conducted periodic reviews. The reviews have resulted in some policy and procedure revisions, which have necessitated additional training. The PMT remains steadfast in their commitment to learn, grow, evolve and assess in order to deliver the most effective privacy program possible.

Let's look at some 2011 accomplishments as well as a look forward to 2012.

A Look Back at 2011

In the past year there has been an increased concern over privacy, partially attributable to the exponential growth and use of social media sites. Without proper precautions, private information can be easily accessed on sites such as Facebook, Twitter and other similar social media forums. We have seen numerous accounts of incidents, breaches and near breaches at the local, state, national and international level. The

heightened media attention has reminded us that the State Privacy Office and Privacy Management Team play an important role in protecting information. Take a look at some of our efforts and achievements from 2011.

BRIM 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 privacy program through financial incentives to agencies within the Executive Branch to complete privacy audits. The 2010 audits asked agencies to certify that they had met the following three criteria: (1) all privacy policies had been implemented, (2) all existing employees had received privacy training, and (3) all laptops with PII or PHI had been encrypted or had a plan in place for encryption. The departments were eager to complete the audits, which resulted in premium reductions of 2% (effective July 2011) for agencies that certified with the State Privacy Office by January 15, 2011.

In 2011, BRIM extended the opportunity for a premium reduction, to take effect July 2012. The audit criteria included the three elements from the previous year, as well as a self-assessment of Notice and Management (Accountability) principles. The self-assessments were completed by Department Privacy Officers (DPOs) and Agency Privacy Officers (APOs), then reviewed and certified by their Department Cabinet Secretaries. The self-assessments and certifications were submitted to the State Privacy Office by November 30, 2011, with a completion rate of 84% by Executive Branch agencies.

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. The many changes included in the HITECH Act created a whole new set of concerns, including significant penalties and increased exposure when breaches occur. These changes prompted the HCA, with input from the PMT, to develop a "HIPAA refresher", which was made available for all covered entities and internal business associates within the Executive Branch. The refresher course was offered through the LMS and remains available for new employees.

Confidentiality Agreements

The PMT took the bold step of deciding that there should be one uniform confidentiality agreement for all Executive Branch employees, and that it should "follow" them as they transfer within the Executive Branch. The PMT embarked on the task of creating a standard confidentiality agreement, with specific departmental addenda as well as the attendant procedure. Focus group meetings were held to review departmental agreements already in use, as well as to discuss components that should be included in all agreements. It was determined that the confidentiality agreement should be delivered online, through the LMS. Each department will decide on the periodicity appropriate for their workforce, and will work with the Office of Technology to include addenda specific to their department.

A Look Forward to 2012

BRIM Self-Assessment

In order to continue auditing our privacy program, four additional criteria will be added to the self-assessment. As in 2011, the self-assessment will be deployed via the LMS, with a similar process for certification. The Chief Privacy Officer will ask the Executive Director of BRIM to consider extending the offer of a premium discount to those departments who complete the assessment.

HIPAA/HITECH

The final HITECH Act regulations are expected in 2012, which will dictate the need for new policy development and revision of the State Government Covered Entities Business Associate Agreement (BAA)[3]. Then, policy training and implementation will take place with the PMT with workforce training occurring thereafter.

Confidentiality Agreements

A standardized confidentiality agreement will be deployed through the LMS in early 2012. Some of the benefits to be derived from the standardized confidentiality agreement include:

- Uniformity of confidentiality agreements across Departments;
- Efficiency in execution;
- Savings due to the process being paperless, and
- Ease of "tracking" to ensure that all employees have signed the agreement.

The associated procedure will be issued in the first quarter of 2012.

Privacy Awareness Refresher

The State Privacy Office is in the process of developing a privacy awareness refresher training to be offered to the Executive Branch workforce. The refresher course is planned for the latter part of 2012.

[3] A Business Associate Agreement is a contract between a covered entity and its associates 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.

Conclusion

In 2011, we witnessed an even greater focus on privacy due, in part, to the growing popularity of social media sites such as Facebook, Twitter and their counterparts. Seldom does a day go by without reading about a privacy concern, incident or breach, whether at the local, state, national or international level. The media focus underscores the importance of the responsibility that the State Privacy Office and the Privacy Management Team are charged with – we are stewards of data. From the inception of the PMT and the Privacy Program, we have sought to develop and administer the best possible privacy program. Throughout 2012, we will continue our journey of discovering, building, communicating and evolving, in order to provide excellence in data stewardship.