West Virginia State Privacy Office

2010 Annual Report

A Report by the State Privacy Office
West Virginia Health Care Authority
December 2010

Executive Branch Departments

- **Governor's Office**
- **Boards and Commissions**
- **Bureau of Senior Services**
- **Department of Administration**
- **Department of Commerce**
- **Department of Education & the Arts**
- **Department of Environmental Protection**
- **Department of Health and Human Resources**
- **Department of Military Affairs & Public Safety**
- **Department of Revenue**
- **Department of Transportation**
- **WV Health Care Authority**

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:

- Implementation of laws, regulations, best practices, policies and procedures to protect PII.
- Protection of citizens' and employees' PII.
- 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, or contact (or impersonate) a particular individual. Personally identifiable information 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); telephone number or fax number dedicated to contacting the individual at their physical place of residence; social security account number; credit and debit card numbers; financial records, including loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints; facial recognition and iris scans; driver identification number; full face image; birth date; birth or adoption certificate number; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet cookie; criminal history, etc. When connected with one or more of the items of information specified above, personally identifiable information 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 Activities – A Look Back

The PMT made significant accomplishments throughout the 2010 calendar year, including the following:

Data Privacy Day: Governor Joe Manchin III proclaimed January 28, 2010 as Data Privacy Day in West Virginia, joining other states, Canada and 27 European countries to raise awareness of data privacy practices and rights.

HIPAA/ARRA Revisited: Building on the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 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 Act) passed on February 13, 2009. The HITECH Act includes 4 parts, one of which is Privacy or Subtitle D. Many of the provisions became 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 PMT participated in several educational sessions to better understand and anticipate the new requirements, including an extensive training for HIPAA covered entities and internal business associates. Additionally, the changes included in the HITECH Act created a need for reassessment of departments' status as a HIPAA covered entity or business associate to a covered entity. This change greatly increased the number of organizations that are required to comply with the HIPAA Privacy Rule. The State Privacy Office coordinated 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 self-evaluated their HIPAA classification and participated in a series of training sessions, developed work plans for compliance, and are prepared to implement in 2011, once the federal regulations are finalized.

Privacy Procedure Revisions: As a result of the HITECH Act, the State Privacy Office issued a revised procedure, *Response to Unauthorized Disclosures*, effective May 21, 2010 and supporting documents to be used in events wherein PII or protected health information (PHI) may have been exposed to unauthorized persons. Among the most significant of the

new HITECH Act mandates is a federal notification requirement for breach of PHI that is not encrypted or otherwise made indecipherable, as well as increasing penalties for violations. Under the HITECH Act, the HIPAA privacy and security rules were strengthened, with business associates now required to comply as if they were covered entities.

Along with the revised procedure, two additional supporting documents, *Generic Breach Notification Letter* and *Privacy Office Post Incident Report,* were updated. The procedure and supporting documents provide for an appropriate response in the event of an unauthorized disclosure of PII or PHI.

In addition to the *Response to Unauthorized Disclosures* procedure, a committee was convened to write procedure for redaction of printed documents. The *Redaction Procedure*, issued in January 2011, provides a basis for appropriate removal of PII and PHI before sharing with a third party. The procedure includes steps which may be taken to ensure that PII and PHI are properly removed, thereby avoiding sanctions, penalties and costs associated with addressing a data breach after the fact.

The HITECH Act also dictated the need to revise the Purchasing Division's Business Associate Agreement and the Notice of Confidentiality, both of which were completed by members of the PMT.

Incident Response Coordination: As noted earlier, the State Privacy Office issued a revision of the *Response to Unauthorized Disclosures* procedure for privacy incidents, and provided training to the PMT members who are HIPAA covered entities and internal business associates within the Executive Branch. The training was very successful and generated much discussion around risk analysis, business associate agreements, notification and post incident reporting.

Executive Branch Policy Implementation and Training Progress: Within the Executive Branch, eleven of twelve organizations did further work in implementing the policies and procedures set forth in the *West Virginia Privacy Program.* Additionally, each of these organizations now requires *Privacy Basics* training for their respective workforce. *Privacy Basics* is an online privacy training program designed to increase awareness of West Virginia Privacy principles and policies. *Privacy Basics* may be accessed via the Office of

Technology's Learning Management System, allowing participants to complete the training in just thirty minutes.

The Department of Administration made strides toward implementing a privacy program, with an Interim Privacy Officer, yet the Privacy Officer position remains vacant and there is additional work to be done.

Department Privacy Officers expressed a desire to improve communication with employees regarding privacy issues, risks and complaints. The State Privacy Office provided the PMT a series of documents which could be used to facilitate communication.

A review of departments' on-line privacy notices revealed that some notices could be improved. A notice is a statement about an organization's privacy and security practices. The Privacy Office made a recommendation for corrective action, including the provision of a template on the PMT website. The recommendation was based on nationally recognized best practices and research regarding making privacy notices readable and understandable to the general public.

During November and December of 2010, the Chapter 30 Licensing Boards embarked on a mission to complete both a *Privacy Assessment* and *Personally Identifiable Information (PII) Checklist*. These tools, once completed, will position the Boards to analyze the data they collect and determine how to protect it from unauthorized access and use. They will implement the privacy policies in 2011.

Privacy Management Team – 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:

Enterprise Initiative 1: In late 2010, a partnership was formed between the West Virginia Health Care Authority (HCA) and the West Virginia Board of Risk and Insurance Management (BRIM). BRIM provides casualty insurance coverage for all State Agencies,

including protection from lawsuits and other liability claims resulting from incidents. In discussions with the Chief Privacy Officer, the Executive Director of BRIM agreed to support the privacy program through financially incentivizing agencies within the Executive Branch to complete privacy audits. The privacy audits may result in premium reductions for agencies who certify that they have met the following three criteria: (1) all privacy policy has been implemented, (2) all existing employees have received privacy training, and (3) all laptops with PII or PHI have been encrypted or have a plan in place for encryption. Agencies who certify with the State Privacy Office by January 15, 2011 will be eligible for a premium reduction in July 2011. Additional audit criteria will be delineated for premium reductions to be granted in 2012. In 2011, a privacy assessment program will be developed to address risks; BRIM financial incentives will encourage participation.

Enterprise Initiative 2: A collaborative encryption effort continues between the PMT and the Governor's Executive Information and Security Team (GEIST). The effort is to ensure that hard drive encryption is in place for laptops which maintain confidential or sensitive data. When an encrypted laptop is stolen or lost, the information remains protected and thus, there is no privacy breach. A challenge was issued by the State Privacy Office to have encryption completed by the end of 2010. Departments rose to this challenge and many met this goal; however, much work does remain to be done.

HIPAA Refresher and HITECH Implementation: 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 need for a "HIPAA refresher" for all covered entities and internal business associates within the Executive Branch. The PMT is in the development process of a refresher training which will incorporate the HITECH Act changes. The training will be deployed to all covered entities and internal business associates in the first quarter of 2011. The final HITECH Act regulations are expected in early 2011, which will dictate the need for new policy development. Policy training and implementation will most likely take place with the PMT in the second quarter of 2011 with workforce training taking place in the summer.

Conclusion

2010 marked a continued focus on Privacy, both at the federal and state levels. The President's HITECH Act continued to create a national privacy and security environment concerned with protections, transparency, and advancement. On the state level, departments embarked on intensive training and education for the workforce with a greater focus on protection of sensitive information and preparation for incident response. Additional procedures were written and disseminated to all State employees, ensuring that they are equipped with the essential tools to guard the PII and legally protected data of the citizens of West Virginia. Collaborative efforts between the Health Care Authority and BRIM, as well as ongoing efforts of the PMT and GEIST provide promise for enhanced protection of the information we will be entrusted with in 2011.