COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **Information Privacy Policy**	Number: **POL-SEC005**
Domain: **Security**	Category:
Date Issued: **06/09/11**	Issued By Direction Of:  Sandra K. Patterson, CIO Bureau of Information Systems
Date Revised: **08/09/2013**	

Table of Contents

1 Introduction

1.1 Purpose

This policy establishes requirements for the collection, use and disclosure of personal information by the Department of Public Welfare (DPW). This policy addresses compliance with Commonwealth of Pennsylvania (CoPA) and federal legal, regulatory and policy requirements related to privacy and information security. Key privacy laws and regulations are identified in the *DPW Information Security and Privacy Policy*. While the collection of personal information is essential to the fulfillment of DPW's mission, the protection of personal information is also a core part of that mission.

1.2 Background

Congress passed the E-Government Act of 2002 to encourage the use of Web-based applications by government agencies as a means of enhancing the quality, effectiveness and efficiency of government operations. The Commonwealth of Pennsylvania (CoPA) has similarly encouraged use of the Internet as a key communication tool. Related to this trend, public concern regarding the disclosure of personal information has increased. To combat this, federal and CoPA legislation has emerged over the last several years that address safeguarding electronic information in a variety of business areas, including health, business, identity and public safety.

Within this context, DPW implements policies and standards to protect the information entrusted to it; while adhering to applicable federal and CoPA privacy and security mandates. Personally identifiable information is information that may be used to identify a specific person; and includes name, address, date of birth, social security number, medical information and financial information.

1.3 Scope

All DPW employees, contractors, and business partners, are responsible for understanding and complying with this policy.

1.4 Compliance

All DPW employees, contractors and other stakeholders are expected to be familiar with and comply with this policy. Violations of this policy may lead to revocation of system privileges and/or disciplinary action. DPW employees who knowingly and willfully violate DPW, Commonwealth or federal law addressing improper use or disclosure of an individual's information may be subject to criminal investigation and prosecution or civil monetary penalties.

1.5 Exemptions

This policy is mandatory for all DPW employees, contractors and business partners. Requests for exemption to the policy should be submitted to the Chief Information Security Officer (CISO). Any exceptions granted will be issued a policy waiver for a defined period of time.

1.6 Policy Review and Update

This document, and its supporting standards and procedures, will be reviewed annually, and updated as needed.

2 DPW Privacy Policy

DPW Policy

General

a. DPW information systems shall meet the appropriate privacy requirements specified by the Health Information Portability and Accountability Act (HIPAA), Internal Revenue Service publication 1075 (IRS 1075), and other federal, state laws and regulations.

Safeguarding Confidential Information - DPW Workplace Practices

b. DPW shall put into place appropriate administrative, physical, and technical safeguards to protect the privacy of personal information, per ITB-PRV001, *Commonwealth of Pennsylvania Electronic Information Privacy Policy*, and other CoPA, federal and industry legal, regulatory and policy requirements.

c. DPW employees, business partners and contractors with access to citizen or business partner information (referred to as "DPW information") shall safeguard personal information from intentional or unintentional use, modification or disclosure.

d. DPW information shall be removed from any electronic media before re-use or disposal, and the data removal shall be documented, per DPW's Media Protection Policy.

e. DPW employees, business partners shall ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.

f. DPW employees, business partners shall ensure that all electronic media (e.g., diskettes, magnetic tapes, USB drives, removable hard drives, compact discs) and hard copy media (e.g., paper, microfilm) are securely stored when their work area is unattended.

Privacy Leadership

g. DPW shall appoint a privacy officer. Roles and responsibilities of the privacy officer are documented in ITB-PRV002, Electronic Information Privacy Officer.

Privacy Impact Assessments

h. A privacy impact assessment (PIA) is required for all DPW information systems that collect, maintain, and/or disseminate DPW information.

Privacy in Systems Development Lifecycle (SDLC)

i. Information systems that are developed to collect, use, share or store DPW information shall meet the guidelines provided in *DPW Web Application Privacy* (STD-ENSS023).

Online Privacy

j. Internal Users of DPW information resources should have no expectation of privacy with respect to the use of those resources, except as otherwise provided by law.

k. External Users of DPW information resources should have the expectation of privacy, except in the case of suspected wrongdoing.

l. DPW may log, review, and otherwise utilize any information stored on or passing through DPW information resources, per DPW's *Audit Logging Policy*.

m. Publicly-accessible DPW web sites, including any such websites operated by contractors on behalf of DPW, must clearly and conspicuously post privacy policies at their principal web sites, at known major entry points to the sites, and at those sites where the agency or the contractor collects substantial personal information from the public.

Data Collection

n. DPW business partners, program offices and vendors shall only collect personally identifiable information when the need for it has been clearly established, per DPW, CoPA, federal and state laws and regulations.

o. DPW business partners, program offices and vendors shall use reasonable efforts to ensure that DPW information is adequately protected from unauthorized disclosure.

DPW Policy

Data Quality

p. DPW employees, contractors, business partners, program offices, system owners and vendors shall establish and implement processes and mechanisms for ensuring that collected personal information is: (1) authentic and accurate, (2) limited to elements required to accomplish the intended purpose of the data collection, (3) complete, and (4) current and not out of date

Notice of Privacy Practices

q. DPW information systems shall provide appropriate privacy disclosure notices to data subjects when personally identifiable information is collected from them. Such disclosures include notice to the individual of the scope, use, dissemination and maintenance of information collected; as well as the right to decline to provide information and to decline consent to the proposed use of the information.

Consent for Secondary Use of Personally Identifiable Information

r. DPW business partners, program offices, system owners and vendors shall use DPW information only for the purpose(s) for which it was collected, unless consent (opt-in) is granted by the individual or the CISO. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected health information for medical research.

Use and Disclosure

s. DPW employees, contractors, business partners, program offices, system owners and vendors shall establish and implement processes and mechanisms for ensuring that access to personal information is limited to those with a need to know. DPW information stored on information systems shall only be accessed by the authorized individual users.

Access to Records and Requests for Corrections

t. DPW business partners, program offices, system owners and vendors shall ensure that clearly communicated processes are in place by which individuals may request access to and amend information relating to them.

Retention and Disposal

u. DPW business partners, program offices, system owners and vendors shall ensure that appropriate data retention practices are in place that meets the requirements of DPW's Media Protection Policy.

Data Breach and Disclosure

v. DPW employees, contractors, business partners and vendors must report with four hours any observed weaknesses in DPW information systems security, any incidents of possible misuse or unauthorized access of DPW information to the CISO, in accordance with DPW's Incident Response and Reporting Policy.

Accountability and Auditing

w. DPW business partners, program offices, system owners and vendors shall develop and implement processes for ensuring accountability for compliance with all applicable privacy protection requirements, including this policy, and all established policies and procedures that govern the collection, use, dissemination, and maintenance of personally identifiable information.

x. DPW business partners, program offices, system owners and vendors shall develop and implement processes for auditing the actual use of personally identifiable information to demonstrate compliance with established DPW privacy requirements.

3 Appendix

3.1 References

Document	Source
DPW Web Application Privacy Standard	DPW
Health Insurance Portability and Accountability Act (HIPAA) Privacy Implementation Handbook	DPW
ITB-PRV001 - Commonwealth of Pennsylvania Electronic Information Privacy Policy	CoPA
ITB-PRV002 - Electronic Information Privacy Officer	CoPA
MD 205.16, Compliance with the Whistleblower Law, Act 1986-169	CoPA
MD 205.36, Right-to-Know Law	CoPA

Policy Revision Log:

Change Date	Version	Change Description	Author and Organization
06/09/2011	1.0	Initial creation	David Johnson
08/09/2013	4.1	Updated	Mathieu Saury