West Virginia Executive Branch
Privacy Policy: **Security Safeguards**

Issued by: Sonia Chambers
West Virginia Health Care Authority

1.0 PRIVACY PRINCIPLE SUBJECT TO THIS POLICY

Security Safeguards – A Department implements the appropriate management, operational, physical and technical controls to preserve the privacy, confidentiality, integrity and accessibility of personally identifiable information (PII). The security safeguards shall be designed to protect the PII from (i) anticipated threats or hazards, and (ii) unauthorized access, use or disclosure. In each case, the Department will strive to provide security that is proportional to the sensitivity of the PII being protected, with the greatest effort being focused on protecting PII from a compromise that could result in substantial harm or inconvenience to the individual.

2.0 POLICY STANDARDS

Each Department shall at all times (i) be in compliance with policies and procedures developed by the Office of Technology (OT) and the Health Care Authority Privacy Office, (ii) securely and economically protect its business functions, including public access to appropriate information and resources, (iii) comply with the legal requirements established by federal and state law and Executive Orders pertaining to confidentiality, privacy, accessibility, and integrity of personally identifiable information. Departments must ensure that nonpublic personal information (NPPI), protected health information (PHI) and sensitive personal information (SPI) is maintained in a secure manner, regardless of format.

2.1 Office of Technology Standards: Departments shall comply with all Office of Technology security requirements as well as requirements imposed by applicable laws and executive orders.

a) Departments shall comply with all OT data classification requirements, and must determine whether they have sensitive data; PII is generally considered sensitive. Departments must work with the Office of Technology to determine if additional controls apply with respect to safeguarding sensitive data.

Examples of Sensitive Personal Information

- Social Security numbers
- Credit card numbers
- Health and Medical data
- Driver license numbers
- Individual financial account numbers

b) Sensitive Personal Information (SPI) may only be disclosed if the disclosure is an "Authorized Disclosure." Authorized Disclosure means a disclosure to:

i) Individuals within the Department who have a business need to know the SPI to conduct Department business.

ii) Third parties who process the SPI on the Department's behalf, such as payroll processors or credit card payment processors, provided that these third parties have a contractual or legal duty to protect the SPI.

iii) Third parties who are qualified commercial or professional entities that provide services to the Department, its customers or employees, such as benefits program providers, provided that these third parties have a contractual or legal duty to protect the SPI.

iv) Third parties who provide legal, accounting and other advisory services to the Department or who are doing research, provided that these third parties have a contractual or legal duty to protect the SPI.

v) Other government agencies, for required reporting purposes.

vi) The individual to whom the SPI pertains or the individual who provided the SPI to the Department (such as to an employee who has provided family-member Social Security numbers for benefits purposes) in accordance with the Individual Rights Policy, and

vii) Any person, if the Department is required by law to make the disclosure (such as in response to subpoenas or court orders) or if the individual to whom the SPI pertains consents to the disclosure.
viii) Third parties receiving information pursuant to the Freedom of Information Act (FOIA).

c) Any disclosure that is not an Authorized Disclosure is an "Unauthorized Disclosure." There are two possible types of Unauthorized Disclosures (1) an ***Internal Unauthorized Disclosure:*** occurs when SPI is exposed or potentially exposed to any person(s) within the Department firewall or Department facilities, and (2) an ***External Unauthorized Disclosure:*** occurs when SPI is exposed or potentially exposed to any person(s) outside the Department firewall or Department facilities. Any known or suspected Unauthorized Disclosure (accidental or otherwise) must be immediately reported to the Department Privacy Officer for appropriate investigation and handling. This reporting requirement applies both to Internal Unauthorized Disclosures and to External Unauthorized Disclosures.

d) Security Incident - A "Security Incident" is any incident that compromises the security, confidentiality, or integrity of PII, with or without SPI. Agencies must implement policies and procedures to ensure that any known or suspected Security Incident (accidental or otherwise) must be immediately reported to the Office of Technology Helpdesk for appropriate investigation and handling.

e) The Department shall implement appropriate procedures to detect and respond to Security threats and Incidents.

Each Department will also establish a process for receiving reports of Unauthorized Disclosures and Security Incidents. This process will (at minimum) include designation of appropriate individuals and resources to:

i) Investigate the incident
ii) Develop and deploy an appropriate, responsive action plan
iii) Notify affected individuals (if applicable) and

iv) Provide recommendations for additional controls or training that may be needed to help prevent a reoccurrence of the incident (if applicable).

2.2 Prohibited Uses of SPI: SPI shall not be collected or used unless reasonably necessary for a specific business purpose, consistent with the Minimum Necessary and Limited Use Policy. SPI shall not be used in any way that generally exposes the information to internal or external persons, unless such exposure is an Authorized Disclosure. The following activities are prohibited (unless a specific law mandates the activity):

i) Government-issued identification numbers (including SSN, Drivers License (DL) numbers) shall not be publicly-posted or displayed.
ii) Social security numbers and driver's license numbers shall not be used as website or phone system user identification numbers (login names) unless the website is encrypted or secure.
iii) Social security numbers and driver's license numbers shall not be printed on materials that are mailed to an individual, unless the Department is legally required to include that number on the document being mailed (such as on tax reporting forms);
iv) Social security numbers and driver's license numbers shall not be printed on any card required for the individuals to access products, services or facilities (such as insurance cards or facility access cards) unless legally required; and,
v) The Department shall not transmit SSN's and DL's (and shall not require an individual to transmit to the Department) Government-issued identification numbers over the internet unless the connection is secure or the SPI is encrypted.

2.3 In addition to the reasonable physical, technical and administrative safeguards to protect SPI required by the OT security program, each Department shall consider the following additional safeguards for SPI:

i) Take reasonable steps to omit SPI on paper reports or printed documents, where possible. If a report must contain SPI, users

should consider whether the SPI can be truncated (such as publishing only partial information).

ii) Take reasonable steps to limit the electronic display of SPI.

iii) Transmit SPI only using secured and/or encrypted methods of transmission approved by the OT.

iv) Store SPI in electronic databases that are access-controlled and store hard-copy SPI in secure physical locations – in each case, limiting access to the SPI to individuals that have a need for such access.

v) Prohibit [Limit] storage of SPI on portable devices (such as laptop computers or removable storage drives) [so that SPI is only on these devices if encrypted or otherwise secured].

vi) Prior to any disclosure of the SPI, verify that the disclosure is an Authorized Disclosure; and

vii) Destroy all documents and electronic media containing SPI in such a way that the information cannot be reconstructed. For example, paper documents may be shredded or burned; electronic media should be overwritten or securely destroyed so that SPI cannot be recovered from the media.

viii) Each Department shall fully comply with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) with respect to all payment card information processed by the Department.

2.4 Network Standards: Network security standards specify the minimum requirements for providing secure interconnection of communications networks and systems while protecting the State's computing resources and information. Departments maintaining their own network infrastructure will comply with the standards approved by the Office of Technology (OT).

2.5 Media Sanitizing and Disposal Standards: Sanitizing and disposal standards protect information assets of the State when a Department decides to redeploy or dispose of IT assets with memory and disk storage capabilities. This includes network devices, computers, mobile devices, and storage media. Departments will comply with the policies developed by the OT.

2.6 Record Retirement and Disposal Standards: Department records in all formats, including paper, are retained or disposed in accordance with the Records Management Procedures developed by the OT. Destruction of records is done in a manner which protects PII from unauthorized disclosure.

2.7 Maintenance Standards: Preventive, periodic maintenance of platform and network infrastructure hardware, operating system software, productivity software, and software applications, including installation of hardware/firmware, software, and application system updates is necessary for security. Departments will comply with the policies and procedures developed by the OT.

2.8 Hard Copy Security: Departments will develop standards [as required by OT] for hard copy security covering all aspects of printers and other multifunction hard copy devices and their usage, including but not limited to: applications, operating system, transmission of the print job or scan job, copying, job hold for user, physical security, device management and user authentication.

2.9 Personnel Security Standards: Personnel will be properly trained to create a proper awareness of the threats, vulnerabilities, and risk reduction strategies in order to protect Department assets and PII. Education will be provided by the OT. Workers handling SPI will be appropriately monitored.

3.0 PROCEDURE

3.1 Departments will comply with policies and procedures developed to assure privacy and security of PII, NPPI and protected health information (PHI).

3.2 Privacy officers will collaborate with the information security administrators and the information security liaisons to support the security program.

3.3 Security incidents will be reported to the OT in accordance with specified reporting requirements. Follow-up activity must comply with the OT security incident response plan and state and federal law.

4.0 PRIVACY REQUIREMENTS

The following laws may impose additional requirements upon Executive Branch Departments with respect to the principle of security safeguards. To the extent these laws may apply to a given Executive Branch Department, legal counsel should be consulted to determine what may apply and in what manner. These laws should be reviewed in conjunction with other applicable state and federal laws, rules, these policies, as well as Department-specific business practices, contracts, or grants. Laws may be in our Privacy Requirements.