

# WEST VIRGINIA DEPARTMENT OF MILITARY AFFAIRS AND PUBLIC SAFETY CONFIDENTIALITY AGREEMENT

---

## OVERVIEW

The purpose of the Confidentiality Agreement is to secure the West Virginia Department of Military Affairs and Public Safety and West Virginia Division of Corrections (Authority's) most protected asset – information. The Authority stores and transmits a great deal of sensitive information. Accordingly, the Authority has concerns about protecting the confidentiality and integrity of this information, in both its paper and electronic forms.

The attached Confidentiality Agreement is being instituted to ensure that all persons with access to protected NPPI, PII, SPII, and PHI information or any other information deemed confidential, fully understand their obligations to limit their use of such information and to protect such information from disclosure. Special attention items, as well as definitions, are highlighted below. If you have any questions about this agreement or fail to understand the contents, please contact personnel for further information.

Special attention items:

- Use of protected NPPI, PII, SPII, and PHI information and confidential information is permitted only when the user has a need to know such information;
- Disclosure of protected NPPI, PII, SPII, and PHI information or confidential information is only permitted when the Authority consents in writing and in conformity with the Authority's policies and procedures, as may be amended from time to time; and
- Protected NPPI, PII, SPII, and PHI information and confidential information is protected in all forms, electronic and paper.

## DEFINITIONS

**Disclosure** – The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

**Need-to-know** – The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.

**WEST VIRGINIA DEPARTMENT OF MILITARY AFFAIRS AND PUBLIC SAFETY  
CONFIDENTIALITY AGREEMENT**

---

---

**Protected Health Information (PHI)** – With regard to HIPAA covered entities, individually identifiable health information, including demographic information, whether oral or recorded in any form or medium, that relates to the individual's health, health care services or supplies, or payment for services or supplies, and which identifies the individual or could reasonably be used to identify the individual. This includes information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual including but not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care as well as counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the health care to an individual; and includes identify information, such as social security number or driver's license number, even if the name is not included, such that the health information is linked to the individual. Protected health information does not include the following:

1. Records covered by the Family Educational Rights and Privacy Act.
2. Employment records held by the entity in its role as employer (although use and dissemination of these records may be subject to other federal and state laws such as the Family and Medical Leave Act and those related to West Virginia Workers' Compensation).

**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 number; credit and debit account 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 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 person physically or electronically.

**Sensitive Personally Identifiable Information (SPII)** – Those elements of PII that must receive heightened protection due to legal or policy requirements.

**WEST VIRGINIA DEPARTMENT OF MILITARY AFFAIRS AND PUBLIC SAFETY  
CONFIDENTIALITY AGREEMENT**

---

---

Sensitive PII includes:

- i. Most data elements in State personnel records
- ii. Occupational licensing data
- iii. Driver history records
- iv. State/Federal contacts data
- v. Employment and training program data
- vi. Permits data
- vii. Historical records repository data
- viii. Personnel data
- ix. Inmate data (IMIS)

Very Sensitive PII includes:

- i. Social Security numbers
- ii. Credit card numbers
- iii. Food assistance programs data
- iv. Criminal history data
- v. Comprehensive law enforcement data
- vi. Foster care data
- vii. Health and Medical data
- viii. Welfare records/data
- ix. Domestic abuse data
- x. Driver license numbers
- xi. Individual financial account numbers
- xii. PREA investigations

Extremely sensitive includes:

- i. State law enforcement investigative records
- ii. Communications systems
- iii. Child and Adult protective services client data

**Non-Public Personal Information (NPPI)** – Any personally identifiable information collected about an individual, including but not limited to, social security numbers, credit card or bank account numbers, medical or educational records, financial information collected by a financial institution used in connection with providing a financial product or service, or other sensitive, confidential or protected data, unless that information is otherwise publicly available.

\_\_\_\_\_ Initial

**WEST VIRGINIA DEPARTMENT OF MILITARY AFFAIRS AND PUBLIC SAFETY  
CONFIDENTIALITY AGREEMENT**

---

---

This agreement, including the attached overview, is entered into between the West Virginia Division of Corrections, a division of the West Virginia Department of Military Affairs and Public Safety (hereinafter DMAPS and both hereafter combined as Authority) and \_\_\_\_\_ (hereinafter the User). The User is considered:

an Employee  a Consultant  a Vendor or  Other, please specify \_\_\_\_\_

WVDOC, DMAPS and the User are jointly referred to as the Parties throughout this agreement.

All of the parties agree as follows:

It is understood between the Parties that during the terms of the User's  Employment,  Contract, or  Other, that the User will only collect such protected Non-Public Personal Information (NPPI), Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), and Protected Health Information (PHI) or other confidential information in conformance with Authority's policy, procedures and rules.

It is also understood between the Parties that during the terms of the User's  Employment,  Contract, or  Other to the extent that the User has a need-to-know such information, the User may have access to protected NPPI, PII, SPII, and PHI or other information deemed confidential, in either paper, electronic or verbal form.

The User agrees not to disclose to anyone, directly or indirectly, any such NPPI, PII, SPII, and PHI or other confidential information, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Authority's policies, procedures, rules, or state or federal law. If information-specific releases, provisions, and restrictions do not exist, then User agrees to disclose confidential information only (1) upon approval of Authority's counsel or designee; and/or (2) with individuals who are known by the User to have prior authorization by their superior to have access to the data or information. All the above applies to the release of information in total or fragmented form. Further, the User agrees not to misuse any media, documents, forms or certificates in any many which might compromise the confidentiality or security, or otherwise be illegal or against Authority's policies, procedures or roles, such as altering a record, using a certificate improperly, etc.

The User understands it is the responsibility of the User to request clarification from the User's immediate supervisor that if there are questions about confidentiality of information or its collection, use or release.

Any document, report, study, article or other written information in whatever format, prepared by the User or information in whatever format that might be given to the User in the course of their  Employment,  Contract, or  Other, and any software, computer equipment, and/or any other property including, but not limited to, copyrighted materials that may be made available from time to time, is the exclusive property of the Authority and shall remain in the Authority's

**WEST VIRGINIA DEPARTMENT OF MILITARY AFFAIRS AND PUBLIC SAFETY  
CONFIDENTIALITY AGREEMENT**

---

---

possession except as otherwise specifically permitted by the Authority. The User understands that all access to information is subject to monitoring and audit.

The User understands that even when the User no longer has access to records of the Authority, the User is still bound by this document and must continue to maintain the confidentiality of information to which access was previously given.

By signing below, the User acknowledges reading and understanding the contents of this document and understands that any improper collection, use or disclosure of NPPI, PII, SPII, and PHI or other information deemed confidential may result in disciplinary action. In addition, the Authority reserves the right to seek any remedy available at law or in equity for any violation of this agreement.

Authority: \_\_\_\_\_

By: \_\_\_\_\_ Its: \_\_\_\_\_

Date: \_\_\_\_\_

User: \_\_\_\_\_

By: \_\_\_\_\_ Its: \_\_\_\_\_

Date: \_\_\_\_\_