WEST VIRGINIA DIVISION OF JUVENILE SERVICES	POLICY NUMBER: 143.00	PAGES: 4
CHAPTER: Administration and Management	**REFERENCE AND RELATED STANDARDS:** WV Code §§ 49-2-903 and 49-5 *et seq.*; ACA 3-JDF-1C-22; Prison Rape Elimination Act (PREA), §115.389; Health Insurance Portability and Accountability Act (HIPAA) of 1996	
SUBJECT: Confidentiality of Information		
DATE: July 1, 2016		

PURPOSE

It is the policy of the West Virginia Division of Juvenile Services to maintain the confidentiality of all juvenile and employee records pursuant to all applicable legal and professional standards.

CANCELLATION

This policy has been revised and supersedes Policy 143.00 dated October 1, 2009.

APPLICABILITY

This Policy applies to all Division of Juvenile Services' facilities, centers and employees.

DEFINITIONS

1. **Confidential Information:** Information that is subject to specific limitations on disclosure. Such information must be specifically labeled, handled, and stored in such a way as to guard against accidental or unauthorized disclosure. All case records are confidential/privileged regardless of the juvenile's age, charges or sentencing court.

2. **Disclosure:** To communicate, transmit, or in any way convey information to any individual or organization in writing, verbal, or other form. Sharing of records between separate Division facilities/centers/units is not considered as disclosure when the information is necessary in the legitimate performance of assigned duties.

3. **Employee**: For the purpose of this policy, an employee shall mean any and all persons working within the West Virginia Division of Juvenile Services including, but not limited to, full time, part time, permanent, temporary, contracted, education and volunteers.

4. **Redact** – To edit or revise by 1) copying a document, 2) blacking out information to be edited on the copy and 3) recopying document. The recopied document is the document that may be released.

PROCEDURES

1. Records that are generated or held by the West Virginia Division of Juvenile Services will be safeguarded and managed pursuant to West Virginia law. Records that are regarded as open to public inspection will be disclosed as prescribed by law.

2. DJS releases information on juveniles only to criminal justice agencies, their staff, and/or other selected agencies, or approved persons on a need-to-know basis in compliance with state statutes, regulations, and applicable federal laws and regulations.

3. Confidentiality of information consists of all orders of commitment, medical and administrative records, applications and reports pertaining to any current or former juvenile in the custody of the Division or any current or former participant in DJS community-based programs. All juvenile information must be kept confidential and may not be disclosed by any person, without approval of the Division and in accordance with law under WV Code §49-5-101 Confidentiality of Records and WV Code §49-5-103 Confidentiality of Juvenile Records.

4. Release of Confidential Information – Personally identifying information about a juvenile who is presently or was previously in the custody of the Division, or who is presently or was previously a participant in a DJS program, may only be disclosed if the juvenile has consented in writing to disclosure. If the juvenile is under age 18, a parent or legal guardian must also grant consent.

5. Subpoena for Juvenile Records – Records should be produced in response to subpoenas which are issued in the following manner:

    a. For a scheduled deposition with a certificate of service or other proof of notice to all parties; or

    b. For actual court hearings and trials.

6. Division employees shall never distribute copies of records to private attorneys or public defenders except where:

    a. They have in their files a written, current authorization for release signed by the person whose records are being released and their attorney; or

    b. They have a court order mandating the release of the records.

7. If a Division employee receives a subpoena, utilizing their chain of command, the employee shall promptly notify the Director and the Legal Department as to the proper response.

8. Release of Information Without the Juvenile's Consent – Confidential information about a juvenile shall be released:

a. Upon request to that juvenile or to his/her parent, guardian, or legal representative. In the case of very sensitive medical or psychological information, the knowledge of which would be potentially harmful to the individual described, the individual is to be referred to the physician or psychologist who was the original source of the record.

b. To the court upon request through proper judicial processes.

c. To authorized persons who are conducting an investigation or criminal proceedings in connection with the administration of a program of the Division. Such investigations include, but are not limited to audits, monitoring and quality control reviews and administrative investigations.

d. To correctional agencies when a proper request has come through the Division via Interstate Compact on Juveniles.

e. To employees of the Division who request the information demonstrating their need for the information in the performance of their regular duties. This includes the release of information to department staff who are providing direct services to that juvenile.

f. To persons outside the Division only when the information is needed for one of the purposes specified above in paragraphs a-e, or it is needed to provide direct services to the individual which are related to the goals and purposes of the Division, and it has been authorized by the Director or the Deputy Director or Designee.

9. The disclosure of case records maintained by the Division on juveniles is governed by WV Code §49-5 *et seq*. These laws provide that records maintained by the Division on juveniles committed to the Division shall not be public records, but shall be privileged records and may be disclosed by the direction of the Director in regard to disseminating juvenile criminal history records only to those persons having a legitimate interest therein.

10. Security of Health Records – Medical information about a juvenile will be maintained according to HIPAA and DJS Policy 165.00-Offender Records. Copies of all mental health documentation are maintained in OIS, as well as any additional information from the juvenile's prior providers (for example, private doctor's statements).

11. If a working file is kept for treatment, mental health or substance abuse information, it must be maintained confidentially and all information must be entered and/or uploaded into OIS in a timely manner and the copy shredded when no longer useful.

12. Sensitive personal information which is potentially damaging to an individual or which may comprise grounds for legal action against the Division if released is to be regarded as confidential. Sensitive information about staff, contract agents, or others may be disclosed or withheld in accordance with law.

13. All employees agree not to disclose to anyone, directly or indirectly, any 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 Division policies, procedures, rules, or state or federal law. If information-specific releases, provisions, and restrictions do not exist, then the employee agrees to disclose confidential information only (1) upon approval of the Division Director and his/her counsel or designee; and/or (2) with individuals who are known by the employee 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 employee agrees not to misuse any media, documents, forms or certificates in any manner which might compromise the confidentiality or security, or otherwise be illegal or against Division policies, procedures or rules, such as altering a record, using a certificate improperly, etc.

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

15. All new employees are required to complete the on-line Privacy Training and sign the West Virginia Executive Branch Confidentiality Agreement (Attachment #1 or can be accessed at www.privacy.wv.gov) within their first two weeks of employment with the Division.

16. This policy will be adopted in its entirety and the facility will not create an operational procedure.

RIGHTS RESERVED

The Director reserves the right to modify, suspend or cancel any provision herein in part or entirety, without advance notice, unless prohibited by law.

APPROVED: _____ 7/1/16

Director **Date**

WEST VIRGINIA EXECUTIVE BRANCH CONFIDENTIALITY AGREEMENT

This Confidentiality Agreement, including any addenda, (collectively this "Agreement") is entered into between the State of West Virginia (the "State") and the undersigned, a member of the Workforce (the "User"). The State and the User are jointly referred to herein as the "Parties".

WHEREAS, the purpose of this Agreement is to secure the Confidential Information the State collects, stores, uses and discloses. Accordingly, the State is concerned with protecting the Privacy, Confidentiality, Integrity and Availability of this information, in its paper, electronic and verbal forms; and

WHEREAS, this Agreement is being instituted to ensure that all members of the Workforce fully understand their obligations to limit their Use of Confidential Information and to protect such information from Unauthorized Disclosure.

NOW, THEREFORE, the Parties agree as follows:

1. Definitions:

a. **Confidential Information** means information that includes, but is not limited to, demographic, medical, and financial information in any form protected by statute or when the release of which would constitute an unreasonable invasion of Privacy, unless the public interest by clear and convincing evidence requires Disclosure in the particular instance, as approved by the designated State counsel or designee. Confidential Information also includes Personally Identifiable Information (PII), as that term is defined below. Confidential Information may be in paper, electronic and verbal forms, and includes images as well as text. Confidential Information includes all information designated confidential by law, rule, policy or procedure, as may be amended from time to time, (collectively referred to herein as "Policy"), such as passwords, client names, trade secrets, information concerning any taxpayer (from any return, declaration, application, audit, investigation, film, record or report) and security audits.

b. **Disclosure** means the release, transfer, provision of access to, sale, divulgence or communication in any other manner of information outside the entity holding the information, in accordance with Policy, as may be amended from time to time.

c. **Need to Know** means the principle that states a User shall only have Access to the minimum information necessary to perform a particular function in the exercise of his or her responsibilities.

d. **Personally Identifiable Information** or **PII** means all information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information (PHI) as that term is defined below. 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.

e. **Protected Health Information** or **PHI** is a subset of PII and means, with regard to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities (*see* 45 C.F.R. §106.103), individually identifiable health information, including demographic information, whether oral or recorded in any form or medium that relates to an individual's health, health care services and 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 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 structure or function of the body; or the past, present, or future payment for the provision of health care to an individual; and which includes identity 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 records covered by the Family Educational Right and Privacy Act, 20 U.S.C. 1232g, and employment records held by the entity in its role as employer.

f. **Use** means the access, utilization, employment, application, examination or analysis of information within an entity that maintains such information.

g. **Workforce** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the State, is under the control of the State, whether or not the State pays them. Workforce does not include Vendors.

h. Any terms not defined herein shall have the definitions afforded them within the Privacy Policy Definitions currently located at www.privacy.wv.gov.

2. Treatment of Confidential Information:

a. The User shall only collect and retain Confidential Information in conformity with Policy.

b. To the extent that the User has a Need to Know Confidential Information, the User may have Access to and shall use such Confidential Information, in conformity with Policy, as may be amended from time to time.

c. The User shall not disclose to anyone, directly or indirectly, any such Confidential Information, unless the individual who is the subject of the Confidential Information consents to the Disclosure in writing or the Disclosure is made pursuant to Policy. At no time shall the Confidential Information be disclosed or used for a personal or non-work-related reason. If information-specific release provisions and restrictions do not exist, then the User shall only disclose Confidential Information (1) upon approval of the designated State counsel or designee; or (2) to individuals who are known by the User to have prior authorization by his or her supervisor to have Access to the information. All of the above applies to release of information in total or fragmented form. When Confidential Information is disclosed, care should be taken to prevent the redisclosure of that information to unauthorized persons or entities. Further, the User shall not misuse any media, documents, forms, or certificates in any manner which might compromise Confidentiality or Security or be otherwise illegal or violate policy, such as altering a record or using a certificate improperly.

d. The User shall protect Confidential Information from unauthorized collection, Use, Access, transfer, sale, Disclosure, alteration, retention or destruction whether accidental or intentional and shall take necessary precautions to secure such Confidential Information to the extent possible.

e. The User is bound by this Agreement and shall continue to protect the Confidential Information to which the User previously had Access, even when he or she no longer has Access to the same, including after termination of the Workforce relationship. The User shall report Incidents pursuant to the Response to Unauthorized Disclosures procedure located at www.privacy.wv.gov.

f. If the User has any questions about this Agreement or the Confidentiality of information or its collection, Use or release, he or she shall request clarification from his or her immediate supervisor or appropriate Privacy Officer.

g. Any document, report, study, article or other written information in whatever format that the User prepares, or information in whatever format that might be given to the User as a member of the Workforce, and any software, computer equipment, or any other property including, but not limited to, copyrighted materials that may be made available from time to time, are the property of the State, or in the custody or control of the State, and shall remain in the State's possession, except as specifically consented to by the State. The User has no ownership rights to or interest in any information owned by or in the custody or control of the State.

h. The User's Access to Confidential Information is at the sole discretion of the State, and may be monitored, audited, modified, suspended, or terminated at any time.

i. The User shall comply with this Agreement and any applicable Privacy or Security policy. Such Compliance is a condition of employment and the User's failure to so comply may subject the User to disciplinary action up to and including dismissal. In addition, the State reserves the right to seek any remedy available at law or in equity for any violation of this Agreement. Further, the User may be subject to civil and criminal penalties for the unauthorized Use or Disclosure of Confidential Information.

Printed Name: _____

Signature: _____

Date: _____