

West Virginia Incident Management System (WVIMS)

User Agreement Policy

This agreement contains an entire understanding between the Bureau for Medical Services (the BMS, Bureau) and the Provider Agency, and supersedes any previous communications, representations, or agreements, verbal or written, related to the subject matter of this Agreement.

This Agreement may not be modified or amended by the Provider Agency in an oral or implied manner, or in any manner which is not set forth in writing, or permitted by this Agreement. This Agreement may, however, be amended by the BMS at any time and without notice.

Any amendments will become effective 30 days, unless circumstances require a change immediately implemented. As a condition, for this Agreement, the Provider Agency agrees to periodically review this Agreement for updates.

1.0 User Requirements

- a. Use of this system may be monitored and reviewed as required for legal, audit, or legitimate authorized operational or management purposes. Users will have no expectation of privacy while using State-provided information resources, and will be required to sign a Statement of Acknowledgement, which recognizes the user has read and agrees to abide by the document. Users may be denied access to information resources if the user fails to execute a signed agreement.
- b. Users must not send or share confidential information for unauthorized purposes.
- c. Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication. All passwords are confidential and **must not** be shared under any circumstances.
- d. Users must not redirect confidential or privileged State data to a non-State owned computing device or PDA without proper authorization.
- e. Confidential, private, personally identifiable information (PII) or sensitive data (i.e. credit card numbers, calling card numbers, logon passwords, PHI, or other protected information), must be encrypted or disassociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.

West Virginia Incident Management System (WVIMS)

User Agreement Policy

- f. Users must immediately contact the BMS at wvims@wv.gov upon receiving or obtaining confidential information to which the user is not entitled (Note: the owner or sender of such information must also be notified) or becoming aware of any inappropriate use of a State-provided IT resource. (See West Virginia Privacy Office procedure#WVEB-P101.1 – *Response to Unauthorized Disclosures*, which accessed at <http://www.privacy.wv.gov>.)
- g. All users have a responsibility to protect data from unauthorized generation, access, modification, disclosure, transmission, or destruction.
- h. The data owner, in conjunction with the designated Bureau individuals, will ensure any confidential data or PII is secured in accordance with applicable federal and state regulations and guidelines.

2.0 User Accounts

- a. The Bureau will administer WVIMS user accounts by adding, modifying, and deleting user access for the Provider Agency. The WVIMS will appoint a designated approval authority, who will authorize all access modifications.
- b. When a user is terminated, the Provider Agency designated approval authority must contact BMS at wvims@wv.gov immediately to disable all access.

3.0 Breach Reporting

- a. As specified by WV State Code and State Privacy Policy, all users of State systems must report suspected or detected information security incidents, as well as all breaches of PHI and/or PII, within 24 hours of discovery.
- b. Because the Bureau and its contractors are supported by WVOT systems and networks, Level 1 security breaches or unauthorized disclosures (see Section 3.4.2.3 of “Breach Reporting”) must be reported by doing one of the following in this preferred order: (1) sending an email to incident@wv.gov with a subject line of “INCIDENT”; (2) going to the WVOT Web Site (<http://technology.wv.gov>), clicking on “Report an Incident,” and filling out an Incident Report Form; or (3) contacting the WVOT Service Desk at servicedesk@wv.gov or by phone at 304-558-9986. All reports must include the following information:
 - Point of contact information for the incident/breach (include name, agency, email address, phone, and cell number(s));
 - Date and time the incident/breach occurred (mm/dd/yy and hh:mm:ss am/pm), if known;

West Virginia Incident Management System (WVIMS)

User Agreement Policy

- What PII or PHI was exposed, if any;
 - A brief summary of the reported incident/breach; and
 - A brief description of the impact of the incident/breach, if known, and
 - Any other information that may be relevant
- c. If the incident involves either a suspected or known breach or disclosure of PHI or PII, the individual must immediately contact the State Privacy Office.

4.0 Violations

- a. Users are accountable for securing all PHI posted and accessible on the Bureau's WV Incident Management System. This means users should **never** give their password to **anyone**, including a *supervisor or manager*, under any circumstances. If a user reveals his/her password to another individual, he/she is violating the West Virginia Computer Crimes and Abuse Act, §61-3C-10, "Disclosure of Computer Security Information."
- b. Users must never disclose the protected health information (PHI) and/or the personally identifiable information (PII) of others, as this is a violation of the Health Insurance Portability and Accountability Act (HIPAA). Based on the nature and extent of the violation, and the nature and extent of the harm resulting from the violation, covered entities and specified individuals who "knowingly" obtain or disclose individually identifiable health information are in violation of the HIPAA. Failure to comply with HIPAA may result in civil and/or criminal penalties in conjunction with Chapter 42 of US Code §1320d-5. User access will be revoked if no record of signed User Agreement Policy exists. The State reserves the right to investigate users suspected of violating federal or state disclosure laws.

West Virginia Incident Management System (WVIMS)

User Agreement Policy

5.0 Acknowledgement

- a. By filling out the below information you acknowledge and agree to adhere to the sections preceding this acknowledgement section

User's Name _____
First Name Middle Initial Last Name

Provider Agency Name _____

Address _____

City _____ State ____ Zip Code _____

Phone _____ Fax _____

E-Mail Address _____

User Signature _____ Date _____

Select one of the following;

☐ Aged & Disabled Waiver ☐ Intellectual/Developmental Disabilities Waiver ☐ Both

Approval Authority's Authorization: I authorize the action indicated above for the specified User to be carried out by the Bureau. I agree to promptly notify the Bureau, by submitting a Request with **Cancel** User indicated when a User no longer has a business purpose to access the information available within the web site.

Provider Agency Approval Signature _____ Date _____

Provider Agency Approval Name _____
First Name Middle Name Last Name