**TABLE OF CONTENTS**



## November 2020

# 1. RIGHT TO PRIVACY/ CONSTITUTIONAL PROTECTION

The Constitution of West Virginia does not provide a general right of privacy.

# 2. KEY PRIVACY LAWS

## 2.1 Personal information breach notification

West Virginia has enacted a personal information breach notification law, under §46A-2A-101 *et seq* of the West Virginia Code ('W.V. Code') ('the Breach Notification Law'). The Breach Notification Law applies to an individual, corporation, business trust, estate, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency or instrumentality, or any other legal entity, whether for profit or not for profit, that owns or licenses computerized data that includes personal information (W.V. Code §46A-2A-101(2)).

Under the Breach Notification Law, a covered entity shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of West Virginia whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of West Virginia. The following definitions are key to understanding whether the law's notification obligations are triggered.

**Breach of the security of a system**: means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure (W.V. Code §46A-2A-101).

**Encrypted**: means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key or securing the information by another method that renders the data elements unreadable or unusable (W.V. Code §46A-2A-101).

**Personal information**: means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: Social Security number; driver's license number or state identification card number issued in lieu of a driver's license; or financial account number, or credit card, or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial accounts. The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public (W.V. Code §46A-2A-101).

**Redact**: means alteration or truncation of data such that no more than the last four digits of a Social Security number, driver's license number, state identification card number or account number is accessible as part of the personal information.

Like most personal information breach notification laws, West Virginia's Breach Notification Law allows notification to be delayed in certain circumstances. In particular, notification may be reasonably delayed if a law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Notice required by this section must be made without unreasonable delay after the law-enforcement agency determines that notification will no longer impede the investigation or jeopardize national or homeland security (W.V. Code §46A-2A-102(e)).

Notification to affected individuals must be provided in writing to the postal address in the records of the individual or entity, by telephone, or by electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures. Alternatively, substitute notice is allowed if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000 or that the affected class of residents to be notified exceeds one hundred thousand persons or that the individual or the entity does not have sufficient contact information or to provide notice. Substitute notice consists of any two of the following: (1) e-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents; (2) conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; or (3) notice to major statewide media (W.V. Code §46A-2A-101(7)).

Notification to affected individuals must include the following (W.V. Code §46A-2A-102(d)):

- to the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including Social Security numbers, driver's licenses or state identification numbers, and financial data;
- a telephone number or website address that the individual may use to contact the entity or the agent of the entity and from whom the individual may learn:
    - what types of information the entity maintained about that individual or about individuals in general; and
    - whether or not the entity maintained information about that individual; and
- the toll-free contact telephone numbers and addresses for the major credit reporting agencies and information on how to place a fraud alert or security freeze.

If notification is provided to more than 1,000 persons of a breach of security, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on a nationwide basis of the timing, distribution, and content of the notices (W.V. Code §46A-2A-102(f)). The Breach Notification Law is enforced by the West Virginia Attorney General ('AG'), who may impose a civil penalty not to exceed $150,000 per breach.

In the event of a personal information breach, organizations are at risk of regulatory enforcement action. For example, the AG has joined multi-state enforcement actions, including the $5 million settlement with Community Health Systems, Inc. in 2020 (which includes $73,897 for West Virginia) and the Equifax settlement in 2019 (which included $2.4 million for West Virginia). In addition, entities are also at risk of civil litigation through West Virginia's General Consumer Protection Laws (see W.V. Code §46A-6-101 et *seq.*).

## 3. HEALTH DATA

### 3.1 Health care records

The West Virginia Health Care Records Law (W.V. Code §16-29-1) requires any licensed, certified, or registered health care provider, upon the written request of a patient or his or her personal representative to furnish a copy of their medical records, in the form of a paper or electronic copy within no more than thirty days from the receipt of the request. Such a request is subject to the following exceptions:

- in the case of a patient receiving treatment for psychiatric or psychological problems, a summary of the record shall be made available to the patient, personal representative, or

his or her authorized agent or authorized representative following termination of the treatment program; and
- the furnishing of a copy, as requested, of the reports of x-ray examinations, electrocardiograms, and other diagnostic procedures shall be deemed to comply.

Notably, the federal Health Insurance Portability and Accountability Act of 1996 ('HIPAA') preempts West Virginia law in the event of a conflict; however, a state law that is more stringent than HIPAA will typically apply (W.V. Code §16-29-1).

### 3.2 AIDS-related medical testing and records confidentiality act

The AIDS-Related Medical Testing and Records Confidentiality Act (W.V. Code §16-3C-3) prohibits any person from disclosing or being compelled to disclose the identity of any person upon whom an HIV-related test is performed, or the results of such a test in a manner which permits identification of the subject of the test, except to the following persons:

- the subject of the test;
- the victim of the crimes of sexual abuse, sexual assault, incest, or sexual molestation at the request of the victim or the victim's legal guardian;
- any person who secures a specific release of test results executed by the subject of the test;
- a funeral director or an authorized agent or employee of a health facility or health care provider if the funeral establishment, health facility or health care provider itself is authorized to obtain the test results, the agent or employee provides patient care or handles or processes specimens of body fluids or tissues and the agent or employee has a need to know that information; provided that the funeral director, agent, or employee shall maintain the confidentiality of the information;
- licensed health care providers or appropriate health facility personnel providing care to the subject of the test;
- the Center for Disease Control and Prevention of the United States Public Health Service in accordance with reporting requirements for HIV and a diagnosed case of AIDS, or a related condition;
- a health facility or health care provider which procures, processes, distributes or uses:
    - a human body part from a deceased person with respect to medical information regarding that person;
    - semen provided prior to the effective date of this article for the purpose of artificial insemination;
    - blood or blood products for transfusion or injection; or

    - human body parts for transplant with respect to medical information regarding the donor or recipient;
- health facility staff committees or accreditation or oversight review organizations which are conducting program monitoring, program evaluation or service reviews so long as any identity remains anonymous;
- claims management personnel employed by or associated with an insurer, health care service contractor, health maintenance organization, self-funded health plan, state-administered health care claims payer, or any other payer of health care claims, where the disclosure is to be used solely for the prompt and accurate evaluation and payment of medical or related claims. Information released under this subsection is confidential and may not be released or available to persons who are not involved in handling or determining medical claims payment;
- persons, health care providers or health facilities engaging in or providing for the exchange of protected health information among the same in order to provide health care services to the patient, including, but not limited to, disclosure through a health information exchange, disclosure and exchange within health care facilities, and disclosure for a permitted purpose, including disclosure to a legally authorized public health authority; and
- a person allowed access to the record by a court order.

Any person aggrieved by a violation of this law has right of action and may recover for the violation against any person who recklessly violates the law, liquidated damages of $1,000 or actual damages, whichever is greater; or against any person who intentionally or maliciously violated a provision of this article, liquidated damages of $10,000 or actual damages, whichever is greater. Such aggrieved person shall also be entitled to reasonable attorney fees and such other relief, including an injunction, as the court may consider appropriate.

## 4. FINANCIAL DATA

### 4.1 Security Freeze Rights

W.V. Code §46A-6L-103 provides that at any time a consumer is required to receive a summary of rights required under Section 609 of the Fair Credit Reporting Act of 1970 ('FCRA'), the following notices must be given:

"West Virginia consumers have the right to obtain a security freeze.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law.

The security freeze will prohibit a consumer-reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer-reporting agency and provide all of the following:

(1) The unique personal identification number or password provided by the consumer-reporting agency;

(2) Proper identification to verify your identity; and

(3) The period of time for which the report shall be available to users of the credit report.

A consumer-reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.

You have the right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer-reporting agency."

Under W.V. Code § 46A-6L-104, if a consumer-reporting agency negligently violates the security freeze by releasing credit information that has been placed under a security freeze, the affected consumer is entitled to:

- notification within five business days following discovery or actual knowledge of the distribution of information, and such notification must include the specific information distributed to third-party and who the recipient of the information was.
- file a complaint with the Federal Trade Commission or the office of the AG.
- file a civil action against the consumer-reporting agency seeking:
    - injunctive relief;
    - actual damages sustained (not more than $1,000, if the violation is willful not more than $5,000); and
    - reasonable expenses, court costs, and attorney's fees.

---

# 5. EMPLOYMENT DATA

## 5.1 Employee's Social Media Accounts

W.V. Code §21-5H-1 provides that an employer shall not do any of the following:

- request, require, or coerce an employee or a potential employee to disclose a username, password, or any other authentication information that allows access to the employee or potential employee's personal account;
- request, require, or coerce an employee or a potential employee to access the employee or the potential employee's personal account in the presence of the employer; or
- compel an employee or potential employee to add the employer or an employment agency to their list of contacts that enable the contacts to access a personal account.

Nothing in this section prevents an employer from:

- accessing information about an employee or potential employee that is publicly available;
- complying with applicable laws, rules, or regulations;
- requiring an employee to disclose a username or password or similar authentication information for the purpose of accessing:
    - an employer-issued electronic device; or
    - an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's busi-

ness purposes.;

- conducting an investigation or requiring an employee to cooperate in an investigation. The employer may require an employee to share the content that has been reported to make a factual determination, if the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data, to an employee's personal account;
- prohibiting an employee or potential employee from using a personal account during employment hours, while on employer time or for business purposes; or
- requesting an employee to share specific content regarding a personal account for the purposes of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct.

If an employer inadvertently receives the username, password, or any other authentication information that would enable the employer to gain access to the employee or potential employee's personal account through the use of an otherwise lawful technology that monitors the employer's network or employer-provided electronic devices for network security or data confidentiality purposes, then the employer is not liable for having that information, unless the employer:

- uses that information, or enables a third party to use that information, to access the employee or potential employee's personal account; or
- after the employer becomes aware that that information was received, does not delete the information as soon as is reasonably practicable, unless that information is being retained by the employer in connection with an ongoing investigation of an actual or suspected breach of the computer, network, or data security. Where an employer knows or, through reasonable efforts, should be aware that its network monitoring technology is likely inadvertently to receive such information, the employer shall make reasonable efforts to secure that information.

Nothing in this section diminishes the authority and obligation of an employer to investigate complaints, allegations, or the occurrence of sexual, racial, or other harassment as provided in this code. Under this section, 'personal account' means an account, service or profile on a social networking website that is used by an employee or potential employee exclusively for personal communications unrelated to any business purposes of the employer.

## 5.2 Employee References

W.V. Code § 55-7-18a shields any employer from civil liability for providing a new prospective employer with adverse or damaging information pertaining to the current or former employee. There is a presumption that the employer is acting in good faith so long as the information they provide to a prospective employer is also provided to an employee in writing at the time of the disclosure. The presumption of good faith may be rebutted upon the showing, by a preponderance of the evidence, that the information disclosed was:

- knowingly false;
- disclosed with reckless disregard for the truth;
- deliberately misleading;
- rendered with malicious purpose toward the former or current employee; or
- disclosed in violation of a nondisclosure agreement or applicable law.

If an employer provides a prospective employer with false or misleading information, upon the employee's request, the employer must give corrected information to all parties that were provided with the false or misleading information.

### 5.3 Employee Monitoring

W.V. Code § 55-7-18a prohibits an employer from using electronic surveillance device or system for the purpose of recording or monitoring the activities of the employees in areas designated for health or personal comfort of the employees. These places include but are not limited to shower rooms, locker rooms, dressing rooms, and employee lounges. Violations of this section is considered a misdemeanor and subject to a five hundred dollar fine. Subsequently, a second offense carries and one thousand dollar fine and a third offense a two thousand dollar fine.

Liability may be imposed on employees for listening to employee's conversations at work. In the case of Bowyer v. Hi-Lad, Inc., 216 W.V. 634, 609 S.E.2d 895, 2004 W.V. LEXIS 197, the court imposed liability on an employer for listening to employee conversations by using hidden microphones in the work area.

## 6. ONLINE PRIVACY

West Virginia does not have any specific laws pertaining to online privacy and online behavioural advertising.

# 7. UNSOLICITED COMMERCIAL COMMUNICATIONS

## 7.1. Unauthorized Electronic Messages

W.V. Code § 46A-6G-2 prohibits any person from:

- transmitting an unauthorized electronic message with the intent to deceive and defraud, or a bulk electronic mail message from a computer located in the state of West Virginia or to an electronic mail address that the sender knows, or has reason to know is held by a West Virginia resident that:
    - uses a third party's internet domain name without the permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path of a commercial electronic mail message;
    - contains false or misleading information in the subject line;
    - does not clearly provide the date and time the message is sent, the identity of the person sending the message, and the return electronic mail address of that person; or
    - contains 'sexually explicit materials,' which are defined as a visual depiction, in actual or simulated form, or an explicit description in a predominately sexual context, nudity, human genitalia, or any act of natural or unnatural sexual intercourse.[1]

A violation entitles an injured party to seek equitable and monetary relief (W.V. Code § 46A-6G-5(b), (c)). The recipient of an unauthorized bulk electronic message may recover for actual damages resulting from the injury sustained. In lieu of actual damages, (W.V. Code § 46A-6G-5(b)) permits a minimum damage assessment of $1,000 for violations. Punitive damages are permitted for an individual's willful failure to cease initiating bulk electronic messages. In addition to monetary damages, the injured party may seek to enjoin the sender of unauthorized bulk electronic messages and, at the discretion of the court, be awarded reasonable attorney fees.

Any interactive computer service provider or public utility injured as a result of a violation of (W.V. Code § 46A-6G-2) may seek monetary relief. Such monetary relief that may be sought by service includes but is not limited to actual damages in the form of loss of profits and attorney fees. In lieu of actual damages, providers may seek statutory damages in the amount of $10 for each and every violation.

## 7.2 Telemarketing Solicitation

W.V. Code §§ 46A-6F-501-601 prohibits telemarketers from engaging in unfair, deceptive, or abusive acts or practices ('UDAAP'). Pursuant to W.V. Code §§ 46A-6F-501-601, UDAAP violations include but are not limited to:

- advertising or representing that registration as a telemarketer equals endorsement by the state;
- engaging in any unfair deceptive conduct which will create a likelihood of confusion;
- engaging in unfair methods of competition;
- initiating outbound calls to a person who previously stated their wish not to receive calls; and
- engaging in telemarketing to a person's residence at any time other than between 8 AM and 9 PM.

The telemarketing provision of West Virginia Consumer Credit and Protection Act applies to those persons who, by any means, initiate or receive telephone calls to or from a customer in West Virginia for the purpose of making a telemarketing solicitation (W.V. Code § 46A-6F-113(a)). Under § 46A-6F-112(a), solicitation includes communication between a telemarketer and a prospective purchaser for the purpose of selling or attempting to sell the purchaser any consumer goods or services. § 46A-6F-201 — 46A-6F-220 includes numerous exemptions for persons or entities that would otherwise fall within the definition of a telemarketer.

Pursuant to W.V. Code § 46A-6F-301, no person shall act as a telemarketer without first registering with the secretary of the Department of Tax and Revenue. The application must be made at least 60 days prior to offering consumer goods or services. Applications for renewal must be made on an annual basis thereafter (W.V. Code § 46A-6F-302) prescribes that the application must be accompanied by a continuing surety bond executed by a corporation that is licensed in the state of West Virginia. Additionally, the bond must be certified before a telemarketer is permitted to conduct business. Failing to meet the registration requirements will subject the telemarketer to a $5,000 fine levied by the Department of Tax and Revenue (W.V. Code §46A-6F-303).

W.V. Code § 46A-6F-410 requires that a telemarketer promptly disclose, in a clear and conspicuous manner:

- The true identity of the telemarketer;
- The purpose of the call is to sell consumer goods or services; and
- The nature of the goods or services offered for sale.

If goods or services are requested by a consumer, before the consumer pays the telemarketer must disclose the quantity, price, and all material aspects of the transaction detailed in W.V. Code § 46A-6F-401(b) 1-7. In regard to sales made, W.V. Code § 46A-6F-402, requires that telemarketers have an accepting returns or canceling services policy in place. The policy at a minimum must allow for at least seven days from the date of delivery the consumer the ability to seek a refund in cash or issuing credit for the purpose. The policy must be disclosed to the consumer orally or via writing. Failing to comply with these sections is considered an unfair deceptive act or practice.

A violation by any telemarketer entitles an individual to initiate an action for monetary damages or equitable relief through an injection. Such monetary damages allowed include actual damages suffered and statutory damages of not less than $100 and no more than $1,000 (W.V. Code § 46A-6F-701(a)). In addition to allowable monetary damages, any sale or lease of consumer goods or services in connection with the violation is void, and the consumer is not required to pay any principal or finance charges. In the instance that the consumer has paid part or all of the cost of goods or services, he or she is entitled to recover such payments (W.V. Code § 46A-6F-701(b)).

W.V. Code § 46A-6F-601(a), (b) provides a safe harbor for telemarketers if they have:

- established and implemented written procedures to avoid outbound telephone calls to persons who have previously stated that that they do not wish to receive such calls;
- trained all of its personnel in such established procedures;
- maintained and recorded lists of persons who have previously stated that they did not wish to receive calls; and
- any violating calls are a result of subsequent error.

W.V. Code §46A-6F-503 provides a prohibition on individuals operating a criminal recovery service. An individual is said to be operating a criminal recovery service when the person:

- makes a representation that he will recover all or any portion of the consideration that a consumer has paid to a telemarketer in response to a telemarketing solicitation;
- does not intend to make such recovery or has no reasonable expectation to anticipate that recovery will be made; and
- receives any remuneration from the consumer before a recovery of consideration is made.

Pursuant to §46A-6F-503, any person who violates this provision is guilty of a felony, and subject to prison sentence of not less than one year and no more than ten years. Additionally, a fine of not more than $5000 will be imposed.

## 8. PRIVACY POLICIES

Currently, West Virginia does not have specific privacy laws or policies. Many of the laws discussed in this analysis include privacy policy requirements, but there is no exclusive law mandating or detailing the applicable standards for such policies. For example, West Virginia's law governing privacy rights and procedures applicable to insurers provides that no insurer shall disclose non-public information of its policyholders unless a specific exemption applies. Such failure on behalf of the insurer to adhere to the privacy requirement subjects them to a $500 penalty and reasonable attorney's fees (W.V. Code Chapter 33).

W.V. Code §16-29G-1 *et seq.* provides that health care providers shall ensure that patient-specific protected health information may be disclosed only in accordance with patient authorization of best interests.

## 9. DATA DISPOSAL/CYBERSECURITY/DATA SECURITY

West Virginia does not have specific data disposal or cybersecurity laws. However, numerous provisions touch on disposal, data security, and what to do in the case of a data breach. For example, W.V. Code § 46A-6F-304, requires telemarketers to keep records produced in telemarketing activities for four years.

The Uniform Electronic Transactions Act (W.V. Code § 39A-1-12) seeks to facilitate electronic transactions consistent with other applicable law. If a particular law requires that a record be retained, the requirement must be satisfied by retaining a record of the information that accurately reflects the information in the record after it was generated, and it must remain accessible for later reference (W.V. Code § 39A-1-12(a)).

### 9.1. Data Breach

Pursuant to W.V. Code § 46A-2A-102(a), West Virginia imposes a duty on individuals or entities that own or license computerized data, which includes personal information, to provide notice of breach of its security system. Upon discovery of a breach, notice is required to be provided to all West Virginia residents without unreasonable delay. Sufficient notice must include (W.V. Code § 46A-2A-102(d)):

- to the extent possible, a description of the categories of information that were believed to be compromised;
- a telephone number or website address that the individual may use to contact the entity or agent of entity to learn of what information may have been compromised, and whether the entity maintained specific information of the individual; and
- the toll-free telephone numbers and addresses for major credit reporting agencies and information on how to place a fraud alert or security freeze on accounts.

In the instance that a data breach puts more than 1,000 individuals at risk, the entity, in addition to notifying all affected parties, must notify all consumer reporting agencies as defined by 15 U.S.C. § 1681a(p). Failure to maintain applicable notice requirements is considered an unfair or deceptive act or practice in violation of this provision and may be enforced by the AG (W.V. Code § 46A-2A-104(b)). Individuals harmed by failure to provide applicable notice have no right to civil remedies unless a court determined that such violations were repeated and willful. In the instance that a court allows an individual to bring a cause of action, such damages are capped at $150,000 per breach of a system or closely related series of breaches.

### 9.2 Cyber Security Program

W.V. Code § 5A-6B-1-6 established the West Virginia Cybersecurity Office, which operates within the state's Office of Technology. The office is under the supervision and control of the Chief Information Security Officer ('CISO'), who shall be appointed by the Chief Technology Officer (W.V. Code § 5A-6B-3(a)). Overall, the CISO is tasked with developing policies, procedures, and standards necessary to establish an effective cybersecurity program for West Virginia Agencies and officials. More particularly, the CISO will conduct cybersecurity risk assessments, provide guidance to particular state agencies and officials, and assist with implementation of cybersecurity framework (W.V. Code § 5A-6B-3(b)(1)-(11)).

## 10. OTHER SPECIFIC JURISDICTIONAL REQUIREMENTS

### 10.1 Student Records and Personal Information

The Student Data Accessibility, Transparency, and Accountability Act (W.V. Code § 18-2-5H), provides numerous privacy protections for students, including but not limited to, restricting transfer and disclosure of student records that contain confidential information, requiring schools to develop privacy plans, and ensuring that all applicable institutions comply with the Federal Family Education Rights and Privacy Act of 1974 ('FERPA').

A school district shall not report to the state the following individual student data (W.V. Code §18-2-5H):

- juvenile delinquency records;
- criminal records;
- medical and health records; and
- student biometric information.

Schools shall not collect the following individual student data (W.V. Code §18-2-5H):

- political affiliation and beliefs;
- religion and religious beliefs and affiliations;
- any data collected through affective computing;
- any data concerning the sexual orientation or beliefs about sexual orientation of the student or any student's family member; and
- any data concerning firearm's ownership by any member of a student's family.

The state superintendent shall appoint a data governance manager, who shall report to and be under the general supervision of the state superintendent. The data governance manager shall have primary responsibility for privacy policy, including (W.V. Code §18-2-5H):

- assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of student data;
- assuring that student data contained in the student data system is handled in full compliance with the Student Data Accessibility, Transparency, and Accountability Act, FERPA, and other state and federal privacy laws;
- evaluating legislative and regulatory proposals involving collection, use, and disclosure of student data by the Department of Education;
- conducting a privacy impact assessment on proposed rules of the state board and department in general and on the privacy of student data, including the type of personal information collected and the number of students affected;
- coordinating with the general counsel of the state board and department, other legal entities, and organization officers to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner;
- preparing a report to the West Virginia Legislature on an annual basis on activities of the department that affect privacy, including complaints of privacy violations, internal controls, and other matters;

- establishing department-wide policies necessary for implementing Fair Information Practice Principles to enhance privacy protections;
- working with the Office of Data Management and Analysis, general counsel, and other officials in engaging with stakeholders about the quality, usefulness, openness, and privacy of data;
- establishing and operating a department-wide Privacy Incident Response Program to ensure that incidents are properly reported, investigated, and mitigated, as appropriate;
- establishing and operating a process for parents to file complaints of privacy violations;
- establishing and operating a process to collect and respond to complaints of privacy violations and provides redress, as appropriate; and
- providing training, education, and outreach to build a culture of privacy across the department and transparency to the public.

The data governance manager shall have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the department that relate to programs and operations with respect to his or her responsibilities under this section and shall make investigations and reports relating to the administration of the programs and operations of the department as are necessary or desirable.

Parents have the right to inspect and review their child's education record maintained by the school and to request student data specific to their child's educational record. School districts must provide parents or guardians with a copy of their child's educational record upon request. Whenever possible, an electronic copy of the educational record must be provided if requested and the identity of the person requesting the information is verified as the parent or guardian

The state board shall develop guidance for school district policies that:

- annually notify parents of their right to request student information;
- ensure security when providing student data to parents;
- ensure student data is provided only to the authorized individuals;
- detail the timeframe within which record requests must be provided;
- ensure that school districts have a plan to allow parents to view and access data specific to their child's educational record and that any electronic access provided is restricted to eligible parties;
- ensure compliance in the collection, use and disclosure of directory information and providing parents or guardians with a form to limit the information concerning their child in directory and subject to release; and
- informing parents of their rights and the process for filing complaints of privacy violations.

Upon the effective date of this section, any existing student data collected by the Department of Education shall not be considered a new student data collection under this section.