HOUSE BILL NO. 634

INTRODUCED BY B. BENNETT

A BILL FOR AN ACT ENTITLED: "AN ACT CREATING THE MONTANA PERSONAL INFORMATION PROTECTION ACT; PROVIDING DEFINITIONS; PROVIDING FOR CONSENT FOR PERSONAL INFORMATION TO BE COLLECTED; PROVIDING FOR COLLECTION, STORAGE, PROCESSING, MODIFICATION, USE, AND DISCLOSURE OF PERSONAL INFORMATION; PROVIDING FOR NOTIFICATION OF COLLECTION OF PERSONAL INFORMATION; PROVIDING FOR SECURITY, ACCIDENTAL DISCLOSURE, AND ACCESS TO PERSONAL INFORMATION; PROVIDING FOR ACCOUNTABILITY AND MAINTENANCE OF SOURCES; PROVIDING FOR REMOVAL AND ERASURE OF INFORMATION; PROVIDING RULEMAKING AUTHORITY; AND ESTABLISHING PENALTIES FOR VIOLATIONS."

WHEREAS, all individuals have a right of privacy in information pertaining to them and the right to privacy is a personal and fundamental right protected by Article II, section 10, of the Montana Constitution, which states that the right of individual privacy "is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest"; and

WHEREAS, the right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies; and

WHEREAS, the increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information; and

WHEREAS, in order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. **Section 1. Short title.** [Sections 1 through 15] may be cited as the "Montana Personal Information Protection Act".

NEW SECTION. **Section 2. Legislative purpose.** The purpose of [sections 1 through 15] is to protect the privacy of Montana citizens. The principles of [sections 1 through 15] include the following:

(1) data subjects must be given notice when their personal information is being collected;

(2) personal information may be used only for the purpose stated and not for any other purposes;

(3) personal information may not be collected or disclosed without the data subject's consent;

(4) personal information that is collected must be kept secure from any potential abuses;

(5) data subjects must be informed as to who is collecting personal information;

(6) data subjects must be allowed to access their personal information and make corrections to any inaccurate data; and

(7) data subjects must have a method available to them to hold data collectors accountable for following the principles contained in this section.

NEW SECTION. **Section 3. Definitions.** As used in [sections 1 through 15], the following definitions apply:

(1) "Agency" means every state office, department, division, bureau, board, commission, or other state or local agency.

(2) "Blocking" means labeling stored personal information in a manner that restricts its further processing or use.

(3) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution. The term includes an entity that disposes of records.

(4) "Collection" means the acquisition of personal information relating to the data subject.

(5) "Communication" means disclosure of personal information either through transmission of the data to the recipient or through the recipient inspecting or retrieving personal information held by the controller.

(6) "Consent" means that the data subject acknowledges and agrees to the collection, processing, and storage of the data subject's personal information according to the terms described in the controller's notification.

(7) "Controller" means any person collecting, processing, using, or disclosing personal information or commissioning others to collect, process, use, or disclose personal information.

(8) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(9) "Data subject" means the individual to whom personal information relates.

(10) "Disclose" means to release, transfer, disseminate, or otherwise communicate all or any part of a record orally, in writing, or by electronic or any other means to any person or entity.

(11) "Entity" includes a business or agency.

(12) "Erasure" means the removal of stored personal information from the controller's system of records in accordance with standard best practices for the medium through shredding, overwriting, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(13) "Governmental entity" means any branch of the federal, state, or local government.

(14) "Individual" means a natural person.

(15) "Modification" means the alteration of the substance of stored personal information.

(16) "Person" means any individual, entity, or agency.

(17) "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including but not limited to an individual's name, signature, social security number, physical characteristics or description, location, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, student loan information, or any other financial information, medical information, or health insurance information. The term includes statements made by or attributed to the individual. Personal information does not include publicly available information that is lawfully made available to the general public.

(18) "Processing" means the storage, modification, communication, blocking, and erasure of personal information.

(19) "Processor" means any entity involved in collection, processing, or use of the personal information on the controller's behalf for the purposes stated by the controller.

(20) (a) "Record" means any medium, regardless of the physical form, on which personal information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.

(b) The term does not include publicly available data containing information that an individual has voluntarily consented to have publicly disseminated or listed.

(21) "Storage" means the entry, recording, or preservation of personal information on a storage medium so that the information can be processed or used again.

(22) "System of records" means one or more records that pertain to one or more individuals, that are maintained by any entity, and that contain personal information.

(23) (a) "Third party" means any person or entity other than the controller of the personal information.

(b) The term does not include the data subject, processors acting on the controller's behalf, contractors acting on the controller's behalf, or persons and bodies commissioned to process or use personal information in relation to [sections 1 through 15].

(24) "Use" means any utilization of personal information other than processing.

NEW SECTION. **Section 4. Consent.** (1) Personal information may be collected, processed, or used by an entity only if the data subject has consented or if [sections 1 through 15] or any other legal provision explicitly permits or allows an activity without the need for consent.

(2) Each entity shall collect, process, or use only that personal information to which the data subject has consented or as required or authorized by the Montana constitution or state law or as mandated by the federal government.

(3) In order to obtain consent, an entity shall first notify the data subject as provided in [section 7].

(4) Consent must be in writing unless special circumstances warrant consent in another form. If consent is to be given together with other written declarations, the declaration of consent must be made distinguishable in its appearance from the other written declarations.

(5) For financial transactions conducted in person, personal information may be collected, processed, stored, or used without the explicit written or verbal consent of the customer for the purposes of completing the financial transaction, retaining an auditable record of the financial transaction, or preventing or investigating fraud. If personal information is collected, processed, stored, or used for the purposes of completing the financial transaction, retaining an auditable record of the financial transaction, or preventing or investigating fraud, the provision of personal information by the customer must be considered consent. The customer must be provided advance notice of collection, processing, and use of personal information through a prominently posted sign or other method as specified in [section 7].

(6) Consent may be given verbally for the purposes of conducting a financial transaction that necessitates the collection, processing, transfer, and disclosure of personal information directly relating to the financial transaction, such as a credit card payment. In this case, notification of collection, processing, transfer, and disclosure must be provided as specified in [section 7].

(7) For identification of an individual in person, an entity may request that an individual provide the individual's name, driver's license number, photograph, address, or similar identifying information for the purpose of identification of the individual by the entity. In this case, the provision of personal information by the individual is considered consent. The individual must be provided advance notice of collection, processing, and use of personal information through a prominently posted sign or other method as specified in [section 7].

(8) When the purpose of collection has been achieved or is no longer relevant, the personal information collected must be erased from the controller's system of records, and from the system of records of all processors.

(9) (a) A data subject who has granted consent has the right to revoke consent at any time. A data subject shall revoke consent in writing by notifying the collector. Upon receipt of a data subject's revocation of consent, the controller shall:

(i) erase the data subject's personal information from the controller's system of records and ensure that it is erased from the system of records of all processors as specified in [section 12];

(ii) notify the data subject in writing when the erasure is complete and verification has been received from all processors.

(b) Erasure must be completed and notification must be sent to the data subject within 60 days after the controller receives the data subject's revocation of consent.

(10) Data subjects may not revoke consent for storage and use of personal information when the personal information was collected for the purposes of maintaining an auditable record of services rendered or products sold and the service has already been provided or the transaction is already complete. Data subjects may revoke consent for this personal information to be used for other purposes only if consent for use for other purposes was granted at the time of collection.

(11) A business may not refrain from conducting commerce with an individual solely because the individual refuses to consent to the business's collection, processing, or use of the individual's personal information except when the personal information is needed for the business to provide the service or product requested, to complete a financial transaction, or to comply with the law. For purposes of this section, securing personal information to conduct credit checks or other fraud prevention measures is not considered necessary for providing the service or product. A business may not charge a higher fee for a product or service solely because an individual refuses to consent to the business's collection, processing, or use of the individual's personal information.

(12) Collection of personal information by the state, an agency, or a political subdivision of the state must comply with the following:

(a) The collection of personal information without consent is permissible only if it is necessary for the state, an agency, or a political subdivision of the state to perform its statutorily or constitutionally mandated duties.

(b) In cases in which personal information is collected without consent, the data subject must be notified in accordance with [section 7] unless notification would be unreasonably detrimental to the purpose for which the personal information is being collected.

NEW SECTION. **Section 5. Collection of personal information.** (1) An entity shall notify the data subject of the collection of personal information in accordance with [section 7]. If consent is not required for collection of personal information, notification must be sent within 14 business days of the collection.

(2) Except as provided in subsection (3), an entity shall collect personal information directly from the individual who is the subject of the information rather than from another source.

(3) Personal information may be collected from a source other than the data subject if:

(a) collection is required by law;

(b) the nature of the administrative duty to be performed necessitates collection of the data from other persons or entities and there are no indications that the interests of the data subject are impaired; or

(c) collection of the personal information from the data subject would necessitate disproportionate effort on the part of the data subject and there are no indications that the interests of the data subject are impaired.

(4) If personal information is collected from the data subject pursuant to law that makes the provision of personal information obligatory or is the prerequisite for the granting of legal benefits, the data subject must be informed that providing personal information is obligatory or voluntary. The data subject must be informed of the relevant statutory or constitutional provision.

(5) When personal information is collected from a private source and not from the data subject, the source must be informed of the legal provision requiring the data subject to provide personal information or that providing the information is voluntary.

NEW SECTION. **Section 6. Storage, modification, processing, and use of personal information.** (1) Storage, modification, processing, and use of personal information may be conducted only if it serves the purpose for which the personal information was originally collected.

(2) Storage, modification, processing, or use of personal information for other purposes is not considered to occur if it is conducted for internal auditing, information security testing and management, or internal organizational process testing and improvement. The provisions of this subsection also apply to processing or use for internal training and examination purposes by the controller unless the data subject has overriding legitimate interests.

(3) Storage, modification, processing, or use for other purposes is permissible only if:

(a) a legal provision requires or peremptorily presupposes use for other purposes;

(b) the data subject has consented;

(c) it is evident that it is in the interest of the data subject and there is no reason to assume the data subject would withhold consent if the data subject was aware of the other purpose;

(d) personal information supplied by the data subject must be checked because there are actual indications that the personal information is incorrect;

(e) the data can be taken from generally accessible sources or the controller would be entitled to publish them unless the data subject clearly has an overriding legitimate interest in excluding the change of purpose;

(f) it is necessary to avert substantial detriment to the common welfare or any other immediate threat to public safety;

(g) it is necessary to prosecute criminal or administrative offenses, to implement criminal sentences or disciplinary measures, or to execute decisions imposing administrative fines;

(h) it is necessary to avert a grave infringement of another person's rights.

(4) Personal information stored exclusively for the purpose of monitoring data protection, safeguarding data, or ensuring proper operation of a data processing system may be used only for those purposes.

NEW SECTION. **Section 7. Notification.** (1) Notice that a data subject's personal information was collected must be provided by one of the methods provided in 30-14-1704(5).

(2) A notice of collection of personal information must include all of the following:

(a) a description of the personal information requested;

(b) the purpose or purposes for which the personal information is being collected and used;

(c) how long the personal information will be stored;

(d) the name of the entity requesting the personal information;

(e) the title, business address, and telephone number of the entity official who is responsible for maintaining the system of records; and

(f) the authority, if any, authorizing the collection, processing, or use of the personal information.

(3) For each item of personal information, the notice must contain:

(a) an explanation of whether submission of the personal information is mandatory or voluntary;

(b) the consequences, if any, of not providing the requested personal information;

(c) any known or foreseeable disclosures of the personal information that may be made; and

(d) the data subject's right of access to records containing personal information that are maintained by the entity.

(4) If written notice is provided pursuant to 30-14-1704(5)(a)(i), the notice must be readily available and in a form that is legible without undue effort on the part of the data subject.

(5) This section does not apply to documents issued by a law enforcement agency when the data subject is provided with an exact copy of the document or to accident reports when the parties of interest may obtain a copy of the report.

NEW SECTION. **Section 8. Disclosure.** (1) (a) Each entity shall notify the data subject of any disclosure of personal information to third parties according to the methods specified in 30-14-1704(5).

(b) If written notice is provided as provided in 30-14-1704(5)(a)(i), the notice must be readily available and in a form that is legible without undue effort on the part of the data subject.

(c) Notice must be provided within 14 days of disclosure.

(2) When the disclosure is of a regularly recurring nature, an initial notice followed by a periodic notice at no more than 1-year intervals is required.

(3) The controller shall provide notice of disclosure upon receipt of a written request by the data subject.

(4) The notice of disclosure must include:

(a) a description of the personal information disclosed;

(b) the purpose or purposes for which the personal information is to be used;

(c) the name of the third party that received the personal information;

(d) the title, business address, and telephone number of the third party official who is responsible for the system of records for use in any future correspondence regarding the personal information that was disclosed;

(e) the authority, if any, allowing the disclosure, processing, or use of the information; and

(f) notice of the data subject's right of access to records containing personal information that are maintained by third parties.

(5) This section does not apply to documents issued by a law enforcement agency when the data subject is provided with an exact copy of the document or to accident reports when the parties of interest may obtain a copy of the report.

(6) Disclosure of any personal information may not be made in a manner that would link the information disclosed to the data subject to whom the personal information relates unless the information is disclosed as follows:

(a) to the data subject;

(b) with the prior written voluntary consent of the data subject obtained not more than 30 days before the disclosure or in the time limit agreed to by the individual in the consent;

(c) to the duly appointed guardian or conservator of the data subject or a person representing the data subject if it can be proven with reasonable certainty through the possession of forms, documents, or correspondence that this person is the authorized representative of the data subject;

(d) to those officers, employees, attorneys, agents, or volunteers of the controller or processor if the disclosure is relevant and necessary in the ordinary course of the performance of official duties and relates to the purpose for which the information was acquired;

(e) with respect to information transferred to or from law enforcement or a regulatory agency, when use of the information requested is needed in the investigation of unlawful activity or for licensing, certification, or regulatory purposes;

(f) to the state, an agency, a political subdivision of the state, the federal government, or a federal agency when required by state or federal law;

(g) to a person or entity who has provided advance, written assurance that the information will be used solely for statistical research or reporting purposes if the information to be disclosed is in a form that will not identify any individual data subject;

(h) pursuant to a determination by an entity that maintains personal information that compelling circumstances exist affecting the health or safety of an individual if, upon disclosure, notification is transmitted to the individual to whom the personal information pertains at the last-known address of the individual. Disclosure may not be made if the disclosure conflicts with state or federal laws.

(i) to the state archives as a record that has sufficient historical or other value to warrant its continued preservation by the state;

(j) to any person pursuant to a subpoena, court order, or other compulsory legal process if before the disclosure the entity reasonably attempts to notify the individual to whom the record pertains and if disclosure is not prohibited by law;

(k) to any person pursuant to a search warrant; and

(l) to a law enforcement agency when required for the investigation of unlawful activity or for licensing, certification, or regulatory purposes unless the disclosure is otherwise prohibited by state or federal law.

NEW SECTION. **Section 9. Security -- accidental disclosure.** (1) Each entity shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of [sections 1 through 15], to ensure the security and confidentiality of personal information, and to protect against anticipated threats or hazards to the security or integrity of personal information.

(2) Any entity that has reason to believe that it has collected or is maintaining personal information in violation of [sections 1 through 15] shall take measures to erase the personal information from its system of records without delay.

(3) When a person or entity has reason to believe that personal information may have been disclosed to a third party in violation of [sections 1 through 15], the person or entity shall notify the controller and the county attorney. Notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in [section 8(6)(l)].

(4) When a controller has reason to believe that personal information may have been disclosed to a third party in violation of [sections 1 through 15], the controller shall notify the data subject as required by [section 8]. Notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in [section 8(6)(l)], or consistent with any measures necessary to determine the scope of accidental disclosure and restore the reasonable security of the system of records.

(5) When there has been any breach or suspected breach of the security of the data system, as defined in 30-14-1704(4)(a), that contains or may contain unencrypted personal information, the data controller shall also follow the requirements of 30-14-1704.

(6) If written notice is provided as provided in 30-14-1704(5)(a)(i), the notice must be readily available and in a form that is legible without undue effort on the part of the data subject.

NEW SECTION. **Section 10. Accountability -- maintenance of sources.** (1) Each entity shall maintain all records containing personal information with accuracy, relevance, timeliness, and completeness to the maximum extent possible.

(2) When an entity transfers a record to a third party, it shall correct, update, withhold, or delete any portion of the record that it knows or has reason to believe is inaccurate or untimely.

(3) Whenever an entity collects personal information, the entity shall maintain the source or sources of the information unless the source is the data subject or the data subject has received a copy of the document, including but not limited to the name of any source who is an individual acting in an individual's own private capacity. If the source is an entity, governmental entity, or other organization, such as a corporation or association, this requirement may be met by maintaining the name of the entity, governmental entity, or organization as long as the smallest reasonably identifiable unit of that entity, governmental entity, or organization is named.

(4) Whenever an entity electronically collects personal information, the entity shall retain a record of the identity of the source, sources, or any intermediate form of the information if either are created or possessed by the entity unless the source is the data subject that has requested that the information be discarded or the data subject has received a copy of the source document.

(5) The entity shall maintain a record of the identity of the source or sources of the information in a readily accessible form in order to provide it to the data subject when the data subject inspects any record pursuant to [section 11]. This section does not apply if the source or sources are exempt from disclosure under the provisions of [sections 1 through 15].

(6) Each entity shall keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made pursuant to [section 8]. The accounting must include the name, title, and business address of the person or entity to whom the disclosure was made. For the purpose of an accounting of a disclosure made under [section 8(6)(l)], it is sufficient for a law enforcement agency to record the date of disclosure, the law enforcement or regulatory entity requesting the disclosure, and whether the purpose of the disclosure is for an investigation of unlawful activity under the jurisdiction of the requesting entity or for licensing, certification, or regulatory purposes by that entity.

(7) Routine disclosures of information pertaining to crimes, offenders, and suspected offenders to law enforcement or to agencies of federal, state, and local government are considered to be disclosures pursuant to [section 8(6)(l)] for the purpose of meeting the requirements of subsection (6).

(8) Each entity shall retain the accounting made pursuant to subsection (6) for at least 3 years after the

disclosure for which the accounting is made.

(9) Nothing in this section may be construed to require retention of the original documents for a 3-year period if the entity is otherwise able to comply with the requirements of this section.

NEW SECTION. **Section 11. Access.** (1) Each individual has the right to inquire and be notified as to whether an entity maintains a record about the individual. Entities shall take reasonable steps to assist individuals in making their requests sufficiently specific.

(2) The data subject's right to information and to erasure as provided in [section 12] or correction as provided in subsections (6) through (8) of this section may not be excluded or restricted by contract.

(3) If the personal information of the data subject is stored in a system of records shared by several entities and the data subject is unable to ascertain the controller of the record, the data subject may approach any of the entities. An entity is required to forward the request of the data subject to the controller of the system of records. The data subject must be informed that the request has been forwarded, and the controller of the record must be identified to the data subject.

(4) Any notice sent to an individual that in any way indicates that the entity maintains any record concerning that individual must include the title and business address of the entity official responsible for maintaining the records, the procedures to be followed to gain access to the records, and the procedures to be followed for an individual to contest the contents of these records unless the individual has received the notice from the entity during the past year. In implementing the provisions of this section, an entity may specify in its rules or regulations reasonable times, places, and requirements for identifying an individual who requests access to a record and for disclosing the contents of a record.

(5) Each entity may establish fees to be charged to an individual for making copies of a record as provided in 2-6-110.

(6) Except as otherwise provided in [sections 1 through 15], each entity shall permit any data subject upon request and proper identification to inspect all the personal information regarding the individual within 30 days of the entity's receipt of the request for active records and within 60 days of the entity's receipt of the request for records that are geographically dispersed or that are inactive and in storage. Failure to respond within these time limits is considered denial. The data subject must be permitted to inspect the accounting made pursuant to [section 10].

(7) The entity shall permit the data subject and, upon the data subject's request, another person of the

data subject's own choosing to inspect all the personal information in the record relating to the data subject and have an exact copy made of all or any portion of the record within 15 days of the inspection. The entity may require the data subject to furnish a written statement authorizing disclosure of the data subject's record to another person of the data subject's choosing.

(8) The entity shall present the information in the record in a form reasonably comprehensible to the general public.

(9) Whenever an entity is unable to access a record by reference to name only or when access by name only would impose an unreasonable administrative burden, the entity may require the data subject to submit other identifying information to facilitate access to the record.

(10) When an individual is entitled under [sections 1 through 15] to gain access to the information in a record containing personal information, the information or a true copy of the record must be made available to the individual at a location near the residence of the individual or by mail, whenever reasonable.

(11) Each entity shall permit a data subject to request in writing an amendment of a record and shall, within 30 days of the date of receipt of a request:

(a) make each correction in accordance with the data subject's request of any portion of a record that the data subject believes is not accurate, relevant, timely, or complete and inform the data subject of the corrections made in accordance with the request; or

(b) inform the data subject of the entity's refusal to amend the record in accordance with the data subject's request, the reason for the refusal, the procedures established by the entity for the data subject to request a review by the head of the entity or an official specifically designated by the head of the entity of the refusal to amend the information, and the name, title, and business address of the reviewing official.

(12) Each entity shall permit any data subject who disagrees with the entity's refusal to amend a record to request a review of the refusal by the head of the entity or an official specifically designated by the head of the entity. The review and a final determination must be completed no later than 30 days from the date on which the data subject requests the review unless, for good cause shown, the head of the entity extends the review period by 30 days. If after a review the reviewing official refuses to amend the record in accordance with the request, the entity shall permit the data subject to file with the entity a statement of reasonable length setting forth the reasons for the data subject's disagreement.

(13) The entity, with respect to any disclosure containing information about which the data subject has filed a statement of disagreement, shall clearly note any portion of the record that is disputed and make available

copies of the data subject's statement and copies of a concise statement of the entity's reasons for not making the amendment to any person or entity to whom the disputed record has been or is disclosed.

(14) [Sections 1 through 15] may not be construed to require an entity to disclose personal information to the data subject if the information:

(a) is compiled for the purpose of identifying individual criminal offenders and alleged offenders and consists only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status;

(b) is compiled for the purpose of a criminal investigation of suspected criminal activities, including reports of informants and investigators, associated with an identifiable individual;

(c) is contained in any record that could identify an individual and that is compiled at any stage of the process of enforcement of the criminal laws, from the arrest or indictment stage through release from supervision and including the process of extradition or the exercise of executive clemency;

(d) is maintained for the purpose of an investigation of an individual's fitness for licensure or public employment, of a grievance or complaint, or of a suspected civil offense if the information is withheld only so that it does not compromise the investigation or a related investigation. The identities of individuals who provided information for the investigation may be withheld pursuant to [section 8(6)(l)].

(e) would compromise the objectivity or fairness of a competitive examination for appointment or promotion, to determine fitness for licensure, or to determine scholastic aptitude;

(f) pertains to the physical or psychological condition of the data subject if the entity determines that disclosure would be detrimental to the data subject. The information must be disclosed, upon the data subject's written authorization, to a licensed medical practitioner or psychologist designated by the individual.

(g) relates to the settlement of claims for work-related illnesses or injuries and is maintained exclusively by the state compensation insurance fund; or

(h) is required by statute to be withheld from the data subject.

(15) This section may not be construed to deny a data subject access to information relating to the data subject if access is allowed by another law of this state.

(16) (a) Except as provided in subsection (16)(c), if the entity determines that requested information is exempt from access, the entity shall inform the data subject in writing of the entity's finding that disclosure is not required by law.

(b) Except as provided in subsection (16)(c), each entity shall, within 30 days from the receipt of a request by a data subject directly affected by the determination, conduct a review of its determination that particular information is exempt from access and shall inform the data subject in writing of the findings of the review. The review must be conducted by the head of the entity or an official specifically designated by the head of the entity.

(c) If the entity believes that compliance with subsection (16)(a) would seriously interfere with attempts to apprehend persons who are wanted for committing a crime or with attempts to prevent the commission of a crime or would endanger the life of an informant or another person submitting information contained in the record, the entity may petition the presiding judge of the superior court of the county in which the record is maintained to issue an ex parte order authorizing the entity to respond to the individual by stating that no record is maintained. All proceedings before the court must be in camera. If the presiding judge finds that there are reasonable grounds to believe that compliance with subsection (16)(a) will seriously interfere with attempts to apprehend persons who are wanted for committing a crime or with attempts to prevent the commission of a crime or will endanger the life of an informant or another person submitting information contained in the record, the judge shall issue an order authorizing the entity to respond to the individual by stating that no record is maintained by the entity. The order may not be issued for longer than 30 days but may be renewed for 30-day intervals. If a request pursuant to this section is received after the expiration of the order, the entity shall either respond pursuant to subsection (16)(a) or seek a new order pursuant to this section.

(17) In disclosing information contained in a record to an individual, an entity may not disclose any personal information relating to another individual that may be contained in the record. To comply with this section, an entity shall, in disclosing information, omit from disclosure information as is necessary. This section may not be construed to authorize withholding the identities of sources except as provided in subsection (14).

(18) In disclosing information contained in a record to an individual, an entity is not required to disclose any information pertaining to that individual that is exempt under [section 8]. To comply with this section, an entity may, in disclosing personal information contained in a record, delete from the disclosure any exempt information.

(19) This section applies to the rights of a data subject to whom personal information pertains and not to the authority or right of any other person or entity to obtain this information.

NEW SECTION. **Section 12. Erasure -- removal.** (1) Upon receipt of a data subject's revocation of consent or when the purpose of collection has been achieved or is no longer relevant, the controller shall ensure that relevant personal information is erased from the controller's system of records and the system of records of all processors within 60 days. The controller shall:

(a) take all reasonable steps to erase the data subject's personal information from the controller's system of records;

(b) notify all processors within 15 days that the data subject's personal information must be removed from their system of records;

(c) receive verification of erasure in writing from all processors acting on the controller's behalf; and

(d) store verification of erasure from all processors for at least 3 years.

(2) Each processor acting on behalf of a controller is required to erase personal information from the processor's system of records and provide written verification to the controller within 30 days of receipt of erasure request from the controller.

(3) Erasure must be conducted by shredding, overwriting, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

NEW SECTION. **Section 13. Organizational policies and procedures -- rulemaking.** (1) Each entity that is a state government agency shall adopt administrative rules specifying procedures to be followed in order to fully implement each of the rights of data subjects established in [sections 1 through 15].

(2) Each entity shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct each person with respect to the rules requirements of [sections 1 through 15], including rules adopted pursuant to [sections 1 through 15] and any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance.

(3) Persons employed in data processing may not process or use personal information without authorization. Before performing the person's duties, a person must be informed of the provisions of [sections 1 through 15] and is required to maintain confidentiality. This requirement continues to be valid after termination of employment.

(4) Each entity involved in collection, processing, or use of personal information shall designate an entity employee to be responsible for ensuring that the entity complies with all of the provisions of [sections 1 through 15].

NEW SECTION. **Section 14. Contracted entities.** (1) A controller may contract a processor to collect, process, use, or disclose records containing personal information on the collector's behalf. The controller is responsible for ensuring compliance with [sections 1 through 15].

(2) The processor must be carefully selected, with particular regard for the suitability of the technical and organizational measures taken to protect and properly manage personal information. The contract shall specify the type of personal information transferred, and the purpose of collection, processing, and use of the personal information, as well as the technical and organizational measures undertaken for compliance with [sections 1 through 15].

(3) The processor shall provide the controller with the title, business address, and telephone number of the entity official who is responsible for the system of records for use in any future correspondence regarding the personal information being disclosed under the provisions of the contract.

(4) The processor may process or use the personal information only as instructed by the controller and in accordance with [sections 1 through 15]. If the processor has reason to believe that an instruction of the controller conflicts with the provisions of [sections 1 through 15] or other data protection provisions, the processor shall notify the controller without delay.

(5) The controller is not required to notify the data subject of disclosures of personal information to processors when the disclosure is undertaken under contract, on behalf of the controller, and in order to accomplish the stated purpose of collection, processing, and use of the personal information.

(6) Within 30 days of receipt of a written request, the controller shall provide the data subject with the names of all processors who have received the data subject's personal information, as well as the title, business address, and telephone number of the corresponding entity official who is responsible for the system of records.

(7) Processors are required to adhere to [sections 1 through 15].

(8) Data subjects have the right to request information, correction, or erasure of their personal information directly from a processor, and the processor shall comply in accordance with [sections 11 and 12].

NEW SECTION. **Section 15. Violations.** (1) A person who willfully, as defined in 1-1-204, requests or obtains any record containing personal information from an entity under false pretenses, bribery, theft, or misrepresentation of identity, purpose of use, or entitlement is guilty of a misdemeanor and shall be fined not more than $5,000 or imprisoned for not more than 1 year, or both.

(2) Except for disclosures that are otherwise required or permitted by law, the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of [sections 1 through

15] is punishable as provided in 50-16-551 and is subject to the civil enforcement and remedy provisions of 50-16-552 and 50-16-553.

(3) A data subject may bring a civil action against an entity if the entity:

(a) refuses to comply with a data subject's request for information pursuant to [section 11];

(b) fails to maintain any record concerning a data subject with the accuracy, relevancy, timeliness, and completeness that is necessary to ensure fairness in any determination relating to the qualifications, character, rights, or opportunities of or benefits to the data subject that may be made on the basis of the record if, as a proximate result of the failure, a determination is made that is adverse to the data subject;

(c) fails to comply with any other provision of [sections 1 through 15] or any administrative rule adopted pursuant to [sections 1 through 15] in a manner that has an adverse effect on a data subject.

(4) (a) In any suit brought under the provisions of this section:

(i) the court may enjoin the entity from withholding the records and order the production to the complainant of any entity records improperly withheld from the complainant. The court may examine the contents of any entity records in camera to determine whether the records or any portion of the records may be withheld as being exempt from the data subject's right of access. The burden is on the entity to sustain its denial of access to the data subject.

(ii) the court may assess against an entity reasonable attorney fees and costs incurred in any suit under this section in which the complainant has prevailed. A party may be considered to have prevailed even though a party does not prevail on all issues or against all parties.

(b) Any entity that fails to comply with any provision of [sections 1 through 15] may be enjoined by any court of competent jurisdiction. The court may make any order or judgment as may be necessary to prevent the use by an entity of any practices that violate [sections 1 through 15].

(5) Actions for injunction under this section may be prosecuted by the attorney general or any county attorney in this state, whether the action is brought upon the attorney general's or county attorney's own complaint, by a member of the general public, or by any individual acting on the individual's own behalf.

(6) In any suit brought under the provisions of subsection (4), the entity is liable to the individual in an amount equal to the sum of:

(a) compensatory and special damages sustained by the individual, including damages for emotional distress; and

(b) the costs of the action together with reasonable attorney fees as determined by the court.

(7) An action to enforce the provisions of [sections 1 through 15] may be brought within 2 years from the date on which the cause of action arises in any court in the county in which the complainant resides or has a principal place of business or where the defendant's records are located. An exception exists when a defendant materially and willfully misrepresents any information required under [sections 1 through 15] to be disclosed to a data subject who is the subject of the information and the information misrepresented is material to the establishment of the defendant's liability to that data subject under [sections 1 through 15]. The action may be brought at any time within 2 years after discovery by the complainant of the misrepresentation.

(8) The rights and remedies provided for in [sections 1 through 15] are nonexclusive and are in addition to those rights and remedies that are available under any other provision of law.

(9) A civil action under this section may not be based upon an allegation that an opinion that is subjective in nature, as distinguished from a factual assertion, about a data subject's qualifications, in connection with a personnel action concerning a data subject, was not accurate, relevant, timely, or complete.

(10) When a remedy, other than those provided in this section, is provided by law but is not available because of a lapse of time, a data subject may obtain a correction to a record under [sections 1 through 15] but a correction may not revise or restore a right or remedy not provided by [sections 1 through 15] that has been barred because of the lapse of time.

NEW SECTION. **Section 16. Codification instruction.** [Sections 1 through 15] are intended to be codified as an integral part of Title 30, chapter 14, and the provisions of Title 30, chapter 14, apply to [sections 1 through 15].

- END -