

4741-1-13

Livestock management practices.

- (A) A person may perform the following livestock production activities: Acts of tagging, ear notching, hoof trimming, deworming, branding, artificial insemination including semen collection, preparation and freezing.
- (B) An owner's agent may perform the following accepted livestock production activities with the advice and consent of a licensed veterinarian who has provided training and oversight consistent with standard herd management practices: castration, tail docking, non-surgical dehorning, intravenous fluid administration, pregnancy detection other than by rectal technique, medication and biological administration, except for those prohibited by law, and phlebotomy.
- (C) For the purpose of this rule, the following definitions apply:
- (1) "Livestock" means an animal produced for fiber, food or other products for human consumption.
 - (2) "Owner's agent" includes a full-time, part-time or seasonal employee of the animal owner. Owner's agent does not include independent or specialty contractors.

Rescind

*** DRAFT - NOT YET FILED ***

4741-1-18

Military exemption.

Veterinarians or registered veterinary technicians serving in the armed forces of the united states shall be exempted from the biennial renewal fee provided written documentation is submitted to the board office evidencing that said licensee is on active duty in the armed forces. Upon receipt of said documentation and submission of the required continuing education hours, the board shall waive the biennial fee and a certificate of renewal shall be issued to the licensee/registrant.

Those licensees/registrants who have been actively engaged in the armed forces of the united states prior to the effective date of this rule shall be exempt from prior renewal fees.

*** DRAFT - NOT YET FILED ***

4741-1-18

Military experience and exemption.

(A) Eligibility for licensee.

In accordance with section 5903. of the Revised Code, the board has determined that there are no military programs of training, military specialties and lengths of service that are substantially equivalent to or which exceed the educational and supervised training requirements for licensure as a veterinarian or a registered veterinary technician.

(B) Definitions related to military service and veteran status.

(1) "Military" in accordance with division (A) of section 5903.03 of the Revised Code, means the armed forces of the United States or a reserve component of the armed forces of the United States, including the Ohio national guard of the national guard of any other state.

(2) "Member" means any person who is serving in the military.

(3) "Veteran" means any person who has completed service in the military and who has been discharged under honorable conditions, or who has been transferred to the reserve with evidence of satisfactory service.

(C) License renewal

(1) Veterinarians or registered veterinary technicians serving in the military shall be exempted from the biennial renewal fee provided written documentation is submitted to the board office evidencing that said licensee is on active duty in the military. Upon receipt of said documentation and submission of the required continuing education hours, the board shall waive the biennial fee and a certificate of renewal shall be issued to the licensee/registrant.

(2) Those licensees/registrants who had been actively engaged in the military during the biennial period and submitted satisfactory evidence to the board of honorable discharge or separation under honorable conditions shall be exempt from the biennial renewal fee for that biennium.

(3) The licensee/registrant may submit an application to the board, stating that the licensee/registrant requires an extension of the current continuing education reporting period because the licensee/registrant has served on active duty during the current or a prior reporting period. The licensee shall submit proper documentation certifying the active duty service and the length of the active duty. Upon receiving the application and proper documentation, the board shall extend the current reporting period by an amount of time equal to the total number of months that the licensee/registrant spent on active duty during the current reporting period. For purposes of this rule, any portion of a month served on active duty shall be considered on full month.

- (4) The board shall consider relevant education, training, or service completed by a licensee/registrant as a member of the armed forces of the United States or reserve components thereof, the Ohio national guard, the Ohio military reserve, the Ohio naval militia, or the national guard of any other state in determining whether a licensee/registrant has fulfilled required continuing education.

*** DRAFT - NOT YET FILED ***

4741-4-01

Definitions.

For the purposes of administrative rules promulgated in accordance with section 1347.15 of the Revised Code, the following definitions apply:

- (A) "Access" as a noun means an instance of copying, viewing, or otherwise perceiving whereas "access" as a verb means to copy, view, or otherwise perceive.
- (B) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as the effective date of the board rule addressing requirements in section 1347.15 of the Revised Code.
- (C) "Board" means the Ohio veterinary medical licensing board.
- (D) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, or retrieves personal information using electronic data processing equipment.
- (E) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the board in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the board confidential.
- (F) "Employee of the state board" means each employee of the state board regardless of whether he/she holds an elected or appointed office or position within the state board. "Employee of the state board" is limited to the Ohio veterinary medical licensing board.
- (G) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.
- (H) "Individual" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.
- (I) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.
- (J) "Person" means a natural person.
- (K) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

- (L) "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code. "System" includes manual and computer systems.
- (M) "Research" means a methodical investigation into a subject.
- (N) "Routine" means commonplace, regular, habitual, or ordinary.
- (O) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to the board's employees and maintained by the board for internal administrative and human resource purposes.
- (P) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.
- (Q) "Upgrade" means a substantial redesign of an existing computer system for the purpose of providing a substantial amount of new application functionality, or application modifications that would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements.

4741-4-02

Procedures for accessing confidential personal information.

For personal information systems, whether manual or computer systems, that contain confidential personal information, the board shall do the following:

- (A) Criteria for accessing confidential personal information. Personal information systems of the board are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the board to fulfill his/her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The board shall establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

- (B) Individual's request for a list of confidential personal information. Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the board, the board shall do all of the following:
 - (1) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;

 - (2) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and

 - (3) If all information relates to an investigation about that individual, inform the individual that the board has no confidential personal information about the individual that is responsive to the individual's request.

- (C) Notice of invalid access.
 - (1) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the board shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the board shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or

national security. Additionally, the board may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system.

"Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once the board determines that notification would not delay or impede an investigation, the board shall disclose the access to confidential personal information made for an invalid reason to the person.

- (2) Notification provided by the board shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.
 - (3) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.
- (D) Appointment of a data privacy point of contact. The board director shall designate an employee of the board to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the board with both the implementation of privacy protections for the confidential personal information that the board maintains and compliance with section 1347.15 of the Revised Code and rules adopted pursuant to the authority provided by that chapter.
- (E) Completion of a privacy impact assessment. The board director shall designate an employee of the board to serve as the data privacy point of contact who shall timely complete the privacy impact assessment form developed by the office of information technology.

4741-4-03

Valid reasons for accessing confidential personal information.

Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the board's exercise of its powers or duties, for which only employees of the board may access confidential personal information (CPI) regardless of whether the personal information system is a manual system or computer system.

Performing the following functions constitute valid reasons for authorized employees of the board to access confidential personal information:

- (A) Responding to a public records request;
- (B) Responding to a request from an individual for the list of CPI the board maintains on that individual;
- (C) Administering a constitutional provision or duty;
- (D) Administering a statutory provision or duty;
- (E) Administering an administrative rule provision or duty;
- (F) Complying with any state or federal program requirements;
- (G) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;
- (H) Auditing purposes;
- (I) Licensure or eligibility for examination purposes;
- (J) Investigation or law enforcement purposes;
- (K) Administrative hearings;
- (L) Litigation, complying with an order of the court, or subpoena;
- (M) Monitoring of disciplinary cases and/or impairment program;
- (N) Human resource matters (e.g. hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);

*** DRAFT - NOT YET FILED ***

4741-4-03

2

- (O) Complying with an executive order or policy;
- (P) Complying with a board policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency; or
- (Q) Complying with a collective bargaining agreement provision.

*** DRAFT - NOT YET FILED ***

4741-4-04

Confidentiality statutes.

The following federal statutes or regulations or state statutes make personal information maintained by the board confidential and identify the confidential personal information within the scope of rules promulgated by this board in accordance with section 1347.15 of the Revised Code;

- (A) Social security numbers: 5 U.S.C. 552a, unless the individual was told that the number would be disclosed.
- (B) "Bureau of Criminal Investigation and Information" criminal records check results: section 4776.04 of the Revised Code.
- (C) Medical Records: Health Insurance Portability and Accountability Act, Title II 45 CFR 160, 42 USC 1320.
- (D) Investigative Records: section 149.43 of the Revised Code.
- (E) College Transcripts: Family Education Rights and Privacy Act, 34 CFR Part 99.

4741-4-05

Restricting and logging access to confidential personal information in computerized personal information systems.

For personal information systems that are computer systems and contain confidential personal information, the board shall do the following:

- (A) Access restriction. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.
- (B) Acquisition of a new computer system. When the board acquires a new computer system that stores, manages or contains confidential personal information, the board shall include a mechanism for recording specific access by employees of the board to confidential personal information in the system.
- (C) Upgrading existing computer systems. When the board modifies an existing computer system that stores, manages or contains confidential personal information, the board shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the board to confidential personal information in the system.
- (D) Logging requirements regarding confidential personal information in existing computer systems.
 - (1) The agency shall require employees of the board who access confidential personal information within computer systems to maintain a log that records that access.
 - (2) Access to confidential information is not required to be entered into the log under the following circumstances:
 - (a) The employee of the board is accessing confidential personal information for official board purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
 - (b) The employee of the board is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.
 - (c) The employee of the board comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group

of specifically named individuals.

(d) The employee of the board accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(i) The individual request confidential personal information about himself/herself.

(ii) The individual makes a request that the board takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(3) For purposes of this paragraph, the board may choose the form or forms of logging, whether in electronic or paper formats.

(E) Log management. The board shall issue a policy that specifies the following:

(1) Who shall maintain the log;

(2) What information shall be captured in the log;

(3) How the log is to be stored; and

(4) How long information kept in the log is to be retained.

Nothing in this rule limits the board from requiring logging in any circumstance that it deems necessary.