4734-3-01 **Confidential personal information.**

(A) Definitions.

(1) "Confidential personal information" means personal information that is not public record for purposes of section 149.43 of the Revised Code.

(2) "Information owner" means the individual directly responsible for the system. The board's information owner is the executive director.

(3) "Personal information" means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.

(4) "System" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved by the name of the person or by some identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment. "System" does not include collected archival records in the custody of or administered under the authority of the Ohio history connection, published directories, reference materials or newsletters, or routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person.

(B) Personal information systems of the board are managed on a need-to-know basis. The executive director determines the level of access required for an employee to fulfill their assigned job duties.

(C) Appointment of a data privacy point of contact. The executive director must designate an employee to serve as the data privacy point of contact to work with the chief privacy officer within the office of information technology to ensure that confidential personal information is properly protected and that the board complies with Chapter 1347 of the Revised Code and rules adopted thereunder. The board's data privacy point of contact shall timely complete the privacy impact assessment form developed by the office of information technology.

(D) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure and log specific access by each employee. Any upgrades to an existing computer system, or the acquisition of a new computer system that stores, manages or contains confidential

personal information, must include a mechanism for recording specific access by employees to confidential personal information in the system.

(E) Valid reasons for authorized employees to access confidential personal information:

(1) Responding to a public records request;

(2) Responding to a request from an individual for a list of confidential personal information maintained on that individual;

(3) Administering a constitutional provision or duty;

(4) Administering a statutory provision or duty;

(5) Administering an administrative rule provision or duty;

(6) Complying with any state of federal program requirements;

(7) Auditing purposes;

(8) Licensure, renewal, reinstatement or restoration processes;

(9) Law enforcement or investigation purposes which may include reviewing confidential personal information of individuals who are not the subject of an investigation, but who otherwise may be witnesses with information related to or pertaining to the investigation.

(10) Administrative hearings;

(11) Litigation, complying with an order of the court, or subpoena;

(12) Human resource matters;

(13) Complying with an executive order or policy;

(14) Complying with an agency policy or a state administrative policy;

(15) Complying with a collective bargaining agreement provision;

(16) Supervising the work of another employee.

(F) Applicable federal or state statutes or administrative rules that make confidential personal information confidential:

(1) Social security numbers: sections 149.43 and 149.45 and U.S.C. 552 (a).

(2) Bureau of criminal identification and investigation criminal records check results: section 4776.04 of the Revised Code.

(3) Medical records: section 149.43 of the Revised Code and Health Insurance Portability and Accountability Act, Title II 45 CFR 160, 42 USC 1320.

(4) Financial and/or medical account numbers: sections 149.43 and 149.45 of the Revised Code.

(5) Law enforcement investigatory records: section 149.43 of the Revised Code and section 4734.45 of the Revised Code.

(6) Educational transcripts: Family Education Rights and Privacy Act, 34 CFR Part 99.

(7) Records excluded by the Ohio Public Records Act: section 149.43 of the Revised Code.

(G) Rights of persons who are subject to personal information. Upon receipt of a signed written request from an individual for a list of confidential personal information about the individual, unless the confidential personal information relates to an investigation about the individual in accordance with sections 149.42 and 4734.45 of the Revised Code, the board must:

(1) Permit the person, the person's legal guardian, or an attorney who presents a signed written authorization made by the person, to inspect all personal information in the system of which the person is the subject;

(2) Inform the person about the types of uses made of the personal information, including the identity of any users usually granted access to the system.

(3) If an individual who is authorized to inspect personal information that is maintained in the system requests a copy of any personal information that the individual is authorized to inspect, the board must provide a copy to the individual.

(H) Notice of invalid access. 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 each person whose information was invalidly accessed in the most expedient time possible, but not later than forty-five days following its discovery or notification of the invalid access, subject to legitimate needs of law enforcement and consistent with measures necessary to determine the scope of the invalid access, including which licensees' personal information was accessed and acquired, and to restore the reasonable integrity of the system.

Replaces: 4734-3-01

Effective:

Five Year Review (FYR) Dates:

_____

Certification

_____

Date

Promulgated Under:	119.03
Statutory Authority:	1347.15
Rule Amplifies:	1347.15
Prior Effective Dates:	10/18/2010, 04/16/2015