Ohio Administrative Code

Rule 4725-13-01 Personal information systems.

Effective: August 30, 2019

(A) The Ohio vision professionals board shall appoint one employee to be directly responsible for the custody and security of each personal information system maintained by the board. Said employee shall:

(1) Inform all employees who have any responsibility for the operation or maintenance of said system or the use of personal information maintained in the system, of the applicable provisions of Chapter 1347. of the Revised Code and rules adopted thereunder; and

(2) Inform all persons requested to supply personal information for a system whether or not he/she is legally required to provide such information; and

(3) Restrict the collection, maintenance and use of personal information to only that which is necessary and relevant to functions of the board as required or authorized by statute, ordinance, code or rule; and

(4) Provide a person, who is asked to supply personal information that will be placed in an interconnected or combined system, with information relevant to the system, including the identity of the other agencies or organizations that have access to the information in the system; and

(5) Allow a person who is the subject of a record in a personal information system to inspect the record pursuant to section 1347.08 of the Revised Code. Upon the request and verification that the person requesting access to the record is the subject of information contained in the system, the employee shall:

(a) Inform the person of any personal information in the system of which he/she is the subject;

(b) Permit the person, or his/her legal guardian, or an attorney who presents a signed authorization made by the person, to inspect all personal information in the system of which he/she is the subject,

except where prohibited by law;

(c) Inform the person of the uses made of the personal information and identify other users who have access to the system;

(d) Allow a person who wishes to exercise his/her rights as provided by this rule to be accompanied by one individual of his/her choice; and

(e) Provide, for a reasonable charge, copies of any personal information the person is authorized to inspect.

(6) Investigate disputes concerning the accuracy, relevance, timeliness or completeness of personal information pursuant to section 1347.09 of the Revised Code and paragraph (D) of this rule; and

(7) Take all reasonable precautions to protect personal information maintained by the Ohio vision professionals board from unauthorized modification, destruction, use or disclosure.

(B) The Ohio vision professionals board shall reprimand in writing any employee who initiates or otherwise contributes to any disciplinary or other punitive action taken against another individual who brings to the attention of appropriate authorities, the press, or a member of the public, any evidence of unauthorized use of any material contained in the personal information system. A copy of the reprimand shall be entered in the employee's personal file.

(C) The Ohio vision professionals board shall monitor its personal information system by:

(1) Maintaining the personal information system with the accuracy, relevance, timeliness, and completeness necessary to assure fairness in any determination made by the board which is based on information contained in the system; and,

(2) Eliminating unnecessary information from the system.

(D) The Ohio vision professionals board shall investigate upon request, the accuracy, relevance, timeliness or completeness of personal information, which is disputed by the subject of a record

contained in the system, within ninety days after receipt of a request from the disputant; and,

(1) Notify the disputant of the results of the investigation and any action the board intends to take with respect to the disputed information; and,

(2) Delete any information that the board cannot verify or finds to be inaccurate; and,

(3) Permit the disputant, if he/she is not satisfied with the determination made by the board to include within the system:

(a) A brief statement of his/her position on the disputed information, such statement being limited to one hundred words with the board's executive secretary assisting the disputant to write a clear summary of the dispute; or

(b) A notation that the disputant protests that the information is inaccurate, irrelevant, outdated, or incomplete; with the Ohio vision professionals board maintaining a copy of the disputant's statement of the dispute.

(E) The Ohio vision professionals board shall not place personal information into an interconnected and combined system, unless said system contributes to the efficiency of the agencies or organizations authorized to use the system in implementing programs which are required or authorized by law.

(F) The Ohio vision professionals board shall not use personal information placed into an interconnected or combined system by another state or local agency or an organization, unless the personal information is necessary and relevant to the performance of a lawful function of the board.

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

(1) "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;

(2) "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;

(3) "Board" means the Ohio vision professionals board;

(4) "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;

(5) "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;

(6) "Employee of the state board" means each employee of a 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 specific employing state board;

(7) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact;

(8) "Individual" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian;

(9) "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;

(10) "Person" means a natural person;

(11) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code;

(12) "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;

(13) "Research" means a methodical investigation into a subject;

(14) "Routine" means common place, regular, habitual, or ordinary;

(15) "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;

(16) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code; and

(17) "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.

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

(1) 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.

(I) 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.

(J) 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.

(a) "Investigation" as used in the above 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.

(K) 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.

(L) 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.

(M) 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.

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

(1) Responding to a public records request;

(2) Responding to a request from an individual for the list of CPI the board maintains 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 or federal program requirements;

(7) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;

(8) Auditing purposes;

(9) Licensure or eligibility for examination processes;

(10) Investigation or law enforcement purposes;

(11) Administrative hearings;

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

(13) Monitoring of disciplinary cases and/or impairment program;

(14) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);

(15) Complying with an executive order or policy;

(16) 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

(17) Complying with a collective bargaining agreement provision.

(O) 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:

(1) Social security numbers: 5 U.S.C. 552 a, unless the individual was told that the number would be disclosed;

(2) "Bureau of Criminal Investigation and Information" criminal records check results: section 4776.04 of the Revised Code;

(3) Medical records: Health Insurance Portability and Accountability Act, Title II 45 CFR 160, 42 USC 1320;

(4) Confidential information obtained during an investigation. Division (C) of section 4725.23 of the Revised Code;

(5) The Family Education Right to Privacy Act (FERPA), 20 U.S.C. 1232 g; and

(6) Ohio Public Records Act. Section 149.43 of the Revised Code.

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

(1) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure;

(2) 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; and

(3) 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.

(Q) 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; or

(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; or

(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.

(R) 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.

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