Ohio Administrative Code

Rule 4729-4-02 Confidential personal information.

Effective: November 1, 2018

(A) 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:

(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 the employee's 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.

(2) 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 the following:

(a) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;

(b) 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

(c) 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.

(3) Notice of invalid access:

(a) Upon discovery of 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 was invalidly 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.

(b) 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.

(c) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

(4) Appointment of a data privacy point of contact. The board executive 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 compliances with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(5) Completion of a privacy impact assessment. The board executive 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.

(B) 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 authorized employees of the board or board members may access confidential personal information (CPI) regardless of whether the personal information system is a manual system or a computer system.

(1) Performing the following functions constitute valid reasons for authorized employees or members 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 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 processes;

(j) Investigation or law enforcement purposes;

(k) Administrative hearings;

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

(m) Human resource matters, including hiring, promotion, demotion, discharge, salary or compensation issues, processing leave requests or issues, time card approvals or issues, and payroll processing;

(n) Complying with an executive order or policy;

(o) 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

(p) Complying with a collective bargaining agreement provision.

(2) To the extent that the general processes described in paragraph (A) of this rule do not cover the following circumstances, for the purpose of carrying out specific duties of the board, authorized employees, contractors and board members would also have valid reasons for accessing CPI in these following circumstances:

(a) Conducting a review of individuals who may be potential witnesses or other sources of information in a criminal or administrative proceeding;

(b) Administering the dangerous drug database also known as the "Ohio Automated Rx Reporting System" or "OARRS";

(c) Inspection purposes;

(d) Administering board orders; or

(e) Research performed for official duties.

(C) Confidentiality statutes, regulations, and rules.

The following federal statutes or regulations or state statutes or administrative rules 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. 552a (12/19/2014), unless the individual was told that the number would be disclosed.

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

(3) Student education records: 20 U.S.C. 1232g (1/14/2013).

(4) Dangerous drug database information: division (C) of section 4729.79 of the Revised Code.

(5) Personal health information: 45 C.F.R. 164.502 (1/25/2013) from the federal "Health Insurance Portability and Accountability Act of 1996 (HIPAA)."

(6) Substance abuse treatment records: section 5119.27 of the Revised Code and 42 U.S.C. 290dd-2 (7/20/2016).

(7) Records of dangerous drugs and controlled substances: section 3719.13 of the Revised Code.

(8) Security or infrastructure records: division (B) of section 149.433 of the Revised Code.

(9) Information or records that are attorney client privileged: division (A)(1) of section 2317.02 of the Revised Code.

(10) Mediation communications or records: section 2710.03 of the Revised Code.

(11) Trial preparation records: division (A)(1)(g) of section 149.43 of the Revised Code.

(12) Court filings: Rule 45(D)(1) of the rules of superintendence for the courts of Ohio.

(13) Section 4729.23 of the Revised Code.

(D) 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:

(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.

(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.

(4) Logging requirements regarding confidential personal information in existing computer systems.

(a) The board shall require employees of the board who access confidential personal information within computer systems to maintain a log that records that access.

(b) Access to confidential information is not required to be entered into the log under the following circumstances:

(i) The employee or contractor 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.

(ii) 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.

(iii) 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.

(c) 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 requests confidential personal information about himself or herself.

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

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

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

(a) Who shall maintain the log;

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

(c) How the log is to be stored;

(d) How long information kept in this log is to be retained.

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