

4731-8-01

Personal information systems.

- (A) All personal information systems of the state medical board shall be maintained in accordance with Chapter 1347. of the Revised Code.
- (B) The executive director of the state medical board shall designate one or more persons to be directly responsible for the personal information systems maintained by the state medical board;
- (C) An employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unauthorized use of information contained in the medical board's personal information systems shall be disciplined at the discretion of the executive director and in a manner which he or she deems appropriate.
- (D) If personal information contained in the medical board's personal information systems is not accurate, relevant, timely, and complete, this fact shall be directed to the attention of the executive director's designee(s), who shall take such action as is deemed appropriate concerning the information system in order to assure fairness in any determination made with respect to the person on the basis of the information.
- (E) The state medical board shall collect only personal information that is necessary and relevant to the functions that the board is required to perform by statute, ordinance, code, or rule. The executive director's designee(s) shall eliminate personal information from the system when it is determined that the information is no longer necessary and relevant to those functions.

4731-8-02

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 of the effective date of the board rule addressing requirements in section 1347.15 of the Revised Code.
- (C) "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.
- (D) "Confidential personal information" 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.
- (E) "Employee" means each employee of the board regardless of whether he/she holds an elected or appointed office or position within the board. "Employee" is limited to the specific employing state agency.
- (F) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.
- (G) "Individual" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.
- (H) "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.
- (I) "Person" means a natural person.
- (J) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.
- (K) "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.

(L) "Research" means a methodical investigation into a subject.

(M) "Routine" means commonplace, regular, habitual, or ordinary.

(N) "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 employees and maintained by the board for internal administrative and human resource purposes.

(O) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

(P) "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.

(Q) "Board" means the "State Medical Board of Ohio."

(R) "Secretary" means the member of the board who is elected under section 4731.02 of the Revised Code to serve as the secretary or a member of the board who is appointed by the board president to act on a temporary basis in lieu of the elected secretary.

(S) "Supervising Member" means the member of the board who is elected under section 4731.02 of the Revised Code to serve as supervising member or a member of the board appointed by the board president to act on a temporary basis in lieu of the elected supervising member.

4731-8-03

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) Establish 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) Respond to an 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) Inform the individual that the board has no confidential personal information about the individual that is responsive to the individual's request if all information maintained by the board relates to an investigation about that individual.

- (C) Notify an individual whose confidential personal information maintained by the board is accessed for an invalid reason.
 - (1) Upon discovery or notification that confidential personal information of an individual has been accessed by an employee for an invalid reason, the board shall notify the individual whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the board shall not

notify the individual if the information is possessed and maintained pursuant to division (F)(5) of section 4731.22 of the Revised Code.

- (a) The board shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation of invalid access or jeopardize homeland or national security.
 - (b) 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 manual or computer system that contains the confidential personal information that was invalidly accessed.
- (2) Notification provided by the board shall inform the individual of the type of confidential personal information accessed and, if known, 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) Appoint a data privacy point of contact. The executive director of the board 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 state of Ohio's 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 the rules adopted pursuant to the authority provided by that chapter.
- (E) Complete a privacy impact assessment. The data privacy point of contact for the board shall timely complete the privacy impact assessment form developed by the office of information technology.

4731-8-04

Valid reasons for accessing confidential person 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 regardless of whether the personal information system is a manual system or computer system:

- (A) Responding to a public records request;
- (B) Responding to a request from an individual for the list of confidential personal information 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 invoices and other financial activities;
- (H) Auditing purposes;
- (I) Licensure, renewal, or verification of licensure processes;
- (J) Investigation or law enforcement purposes;
- (K) Administrative hearings or evidentiary review by a hearing examiner;
- (L) Litigation, complying with an order of the court, or subpoena;
- (M) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues, payroll, Federal Medical Leave Act issues, disability issues, employee assistance program issues);
- (N) Complying with an executive order or policy;
- (O) Complying with a board policy or resolution, or with a state administrative policy or

directive issued by the department of administrative services, the office of budget and management or other similar state board;

(P) Complying with a collective bargaining agreement provision;

(Q) Administering a board program;

(R) Facilitating operational efficiencies or responding to complaints about the board's investigative, monitoring, or licensure processes; or

(S) Maintaining data systems or performing information technology responsibilities.

4731-8-05

Confidentiality statutes.

With regard to confidential personal information maintained by the board, the following federal statutes or regulations or state statutes and administrative rules make the personal information confidential:

- (A) Social security numbers of applicants, licensees, and board employees: 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) Complaints, the names of complainants and patients, and information received in an investigation, including any medical records of the subject of the complaint: division (F) of section 4730.26, division (F) of section 4731.22, division (E) of section 4760.14, division (E) of section 4762.14, and division (E) of section 4774.14 of the Revised Code.
- (D) Medical malpractice payouts reported by a professional liability insurer: division (F) of section 4730.32, division (F) of section 4731.224, division (F) of section 4760.16, division (F) of section 4762.16, and division (F) of section 4774.16 of the Revised Code.
- (E) Formal disciplinary action reported by a health care facility: division (F) of section 4730.32, division (F) of section 4731.224, division (F) of section 4760.16, division (F) of section 4762.16, and division (F) of section 4774.16 of the Revised Code.
- (F) A belief that a violation of law has occurred when reported by a licensee or professional society of licensees: division (F) of section 4730.32, division (F) of section 4731.224, division (F) of section 4760.16, division (F) of section 4762.16, and division (F) of section 4774.16 of the Revised Code.
- (G) Medical records of board employees or their family members: "Family Medical Leave Act of 1993," Pub. L. No. 103-3; 29 U.S.C. Sec. 260 as implemented in 29 C.F.R. 825.500; Section I of the "Americans with Disabilities Act of 1990," 42 U.S.C. Sec. 12112(d).
- (H) Employee assistance program records: section 124.88 of the Revised Code.
- (I) Alcohol and drug treatment records: 42 CFR Part 2; 42 U.S.C. 290dd-3.
- (J) "Federal Bureau of Investigation" criminal records check results: section 4776.04 of the Revised Code; 28 CFR 20.33(d).

(K) “National Practitioner Data Bank” and “Healthcare and Integrity Protection Data Bank” reports: 45 CFR Part 60.

(L) Residential and familial information for covered licensees: sections 149.43(A)(1)(p), 149.43(A)(7), and 149.43(A)(8) of the Revised Code.

4731-8-06

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 restrictions. 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 makes an upgrade to a computer system, as that term is defined in rule 4731-8-02 of the Administrative Code, to an existing computer system that stores, manages or contains confidential personal information, the upgrade 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) Employees who access confidential personal information within computer systems shall maintain a log that records that access.
 - (2) Access to confidential information is not required to be entered into a log under the following circumstances:
 - (a) The employee 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 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 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 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/herself; or

(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 that request.

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

(1) The form or forms for logging;

(2) Who shall maintain the logs;

(3) What information shall be captured in the logs;

(4) How the logs are to be stored; and

(5) How long information kept in the logs is to be retained.

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