CONFIDENTIAL PERSONAL INFORMATION POLICY (2019-02)

It is the policy of the board to restrict access to non-public personal information to only those employees who need access to perform a specific legitimate governmental objective on behalf of the board. Legitimate governmental objectives of the board include those functions set forth in sections 4725 of the Revised Code and in Chapter 4725 of the Administrative Code including, but not limited to, investigation of information related to violations of the above-referenced sections of the Revised Code or rules adopted by the board; adjudication of disciplinary actions; monitoring the compliance of individuals under consent agreement; processing initial applications for, or renewal of licensure; survey, review and/or approval of continuing education programs via continuing education audits.

(A) Authority

The 127th General Assembly, through HB 648, enacted section 1347.15 of the Revised Code. R.C. 1347.15 requires all state agencies to adopt rules, policies, and procedures that regulate employees' access to confidential personal information kept by the agency.

(B) Application and Scope

The policy applies to all records kept by the board, whether in electronic or paper form. Likewise, the policy applies to all employees of the board and to all persons who are granted access, for valid business reasons, to the records of the board that may contain confidential personal information.

(C) Definitions

As used in Revised Code section 1347.15 and in the policy, the following definitions apply:

(1) "Confidential personal information" means personal information that is not a public record for purposes of section 149.43 of the Revised Code. Information includes a social security number, a criminal record check result, or a disciplinary file. For the purpose of the policy, it is intended that the term "confidential personal information" includes "sensitive personal information" as defined in the Governor's November 20, 2008 Management Directive.

(2) "Personal" refers to information about a natural person or individual as used in section 1347.12 (A)(2)(b)(5) of the Revised Code.

(3) "State agency" does not include the courts or any judicial agency, and state-assisted institution of higher education, or any local agency; and

(4) "Records" has the same meaning as set forth in section 149.011 (G) of the Revised Code.

(4) "System" means any collection or group of information including, but not limited to, electronic or paper files, databases, or any externally accessed source not under direct control of the board.

Procedures

(A) Criteria for Access to Confidential Personal Information

ORC 1347.15 (B)(1) requires that every state agency, including the board, develop criteria for determining which of its employees may have access to confidential personal information, and which supervisors may authorize those employees to have access. Employees of the board shall maintain confidentiality regarding confidential personal information acquired while employed by the board, including, but not limited to, social security numbers of applicant/licensee/registration holders and board employees and information obtained in the course of an investigation, including patient records contained in investigative files. Confidentiality must be maintained both during and after employment with the board as required by Ohio Ethics Law. Access to confidential personal information shall be granted at the lowest level necessary that allows for an individual to perform their assigned duties in order to minimize the potential impact to the public. For the board, the following criteria apply:

(1) The Executive Director, Board Investigator, Administrative Professionals, and other authorized staff may have unlimited access to any and all confidential personal information in the possession of the board.

(2) The Executive Director, Board Investigator, Administrative Professionals, and other authorized staff may have unlimited access to any and all confidential personal information contained in the eLicense Ohio System; and, paper files related to individuals licensed by the board; and, individuals applying for licensure with the board; and, access to any and all confidential personal information contained in OAKS; or, the paper personnel files for all employees and board members.

(3) All board members may have unlimited access to any and all confidential personal information contained in the Ohio e-Licensing System and paper files related to individuals applying for licensure and personnel files for all staff employed by the board.

(4) Any board member serving on an Investigative Review Group panel may have unlimited access to any and all confidential personal information contained in disciplinary files related to alleged violation of the laws regulating the practice of the Ohio Vision Professionals Board.

(5) All board employees are entitled to access their own OAKS information and all other confidential personal information kept on file for payroll and other time and hour functions.

(6) Access to electronically stored data shall be granted using assigned passwords that expire after not less than 60 days.

(B) Rational Access to Confidential Personal Information

Board employees are only permitted to access confidential personal information that is acquired by or in the possession of the agency for valid business reasons. Specifically, "valid business reason" are those reasons that reflect the employee's execution of the duties of the Board as set for in sections 4725 of the Ohio Revised Code; and, Chapters 4725 of the Ohio Administrative Code. Employees are also permitted to access their individual employment records, which contain confidential personal information, for time and hour and other payroll reasons.

(C) Statutory and Other Legal Authority for Confidentiality

The term "confidential personal information" is defined by Revised Code sections 1347.15 and 149.43. Other state and federal statutes, and even case law, may add to the collection of information that is classified as "confidential personal information" (see, e.g.:*The Health Insurance Portability and Accountability Act of 1996 [HIPAA], which makes confidential certain health information, or State ex rel. office of Montgomery city Public Defender v. Siroki (2006), 108 Ohio St.3d 207, 2006-Ohio-662, concerning social*

security numbers). An exhaustive list cannot be attached. Consequently, board employees should contact the Executive Director before accessing a record if they are unsure if it contains confidential personal information. In addition, some personal information and records may be deemed confidential when received or generated by the board pursuant to an investigation and are not public records as defined in section 149.43 of the Revised Code and 4725.23 in the Administrative Code and are not subject to discovery in any civil or administrative action.

(D) Existing Computer Systems and Computer Upgrades

In the event that the board intends to upgrade its existing computer system or purchase any new computer system that stores, manages, or contains confidential personal information, the new system and/or upgrades shall contain a mechanism for recording specific access by employees of the board to the confidential personal information. Until an upgrade or new acquisition of such a computer system is made, employees accessing confidential personal information should keep a log that records access of the confidential personal information.

(E) Requests for Information from Individuals

The board may receive requests from individuals who want to know what confidential personal information is kept by the board. Only written requests will receive a response. However, board employees receiving such a request should consult with the Executive Director before any response is provided. Under no circumstances will the subject of an investigation be provided with information about the confidential personal information the board has pertaining to that individual.

(F) Access for Invalid Reasons

Even though appropriate safeguards are in place for protecting the confidentiality of personal information, it is possible that an employee of the board might gain access to such information for invalid reasons. Should an incident of invalid access occur, the Executive Director will advise the individual whose information was invalidly accessed of the breach of confidentiality as soon as is reasonably possible. However, if such notice would compromise the outcome of an investigation, notice may be provided upon completion of the investigation.

(G) Data Privacy Point of Contact

By law, the board must appoint a data privacy point of contact. That individual will work with the State's Chief Privacy Office to ensure that confidential personal information is properly protected and that the requirements of R.C. 1347.15 are satisfied. The data privacy point of contact will be responsible for completing a privacy impact assessment form(s) for the board. The Executive Director shall serve as the board's data privacy point of contact.

(H) Use of Authentication Measure

Every board employee is required to have a personal and secure password for a computer. Through that computer, the employee may be able to access confidential personal information. Board employees are to keep passwords confidential and are prohibited from using their own passwords to log onto systems for non-employees or other persons.

(I) Training and Publication of Policy

The board will develop a training program for all its employees so that those employees are made aware of all the rules, laws, and policies governing their access to confidential personal information. In addition, the policy will be copied and distributed to each board employee. Employees will acknowledge receipt of the copy in writing. Amendments to the policy will be distributed and acknowledged in the same way. Further, a copy of the policy will be prominently posted in a conspicuous place in the board office and posted on the board's website.

(J) Disciplinary Measures for Violations

No employee of the board shall knowingly access, use, or disclose confidential personal information for reasons that would violate the policy. Knowingly accessing, using or disclosing confidential personal information in violation of the policy is a first-degree misdemeanor, is cause for immediate termination from employment, and is cause for prohibition on employment with the State. Disciplinary actions including termination cannot be negotiated in state collective bargaining agreements.

(K) Attestation Log

Employees shall sign an attestation log to document the employee's ongoing compliance with the policy and the appropriate access and handling of confidential personal information. Log Forms, attachment A, will be maintained by the Executive Director/Data Privacy Point of Contact (DPPOC).

Effective May 16, 2019

Attachment A: Confidential Personal Information Attestation Log (2019-02)

PRINT EMPLOYEE NAME	DATE RECEIVED	DATE READ	EMPLOYEE SIGNATURE

Ohio | Ohio Vision Professionals Board

Confidential Personal Information Attestation Log (2019-02)

PRINT EMPLOYEE NAME	DATE RECEIVED	DATE READ	EMPLOYEE SIGNATURE
Dr. Chery Archer	5/16/19	5/16/19	Cheryl Archer
Thomas Barracato	5/16/19	5/16/19	
Dr. Jacqueline Davis	5-16-19	5-16-19	
Dr. Darrell Dye	5-16-19	5-16-19	
Kimberly Mermis	5-16-19	5-16-19	
Brian Miller	16 May 2019	16 may 2019	
Dr. Thomas Nye	5/16/2019	5/16/2019	
Marlene Anielski	5/15/19	5/15/19	
Dave Bailey	5-16-19	5-16-19	
Adela Lopez-Wellman	5/16/19	5/16/19	
Wilma Simmons	5-16-19	5-16-19	