Access to Confidential Personal Information Policy *Executive Director Approved Work Rules*	
Executive Director	
Effective Date	April 20, 2009 Revised January 3, 2011 Revised September 12, 2013

POLICY:

(A) Authority

In late 2008, in response to the "Joe the Plumber" case, 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) Purpose

This policy is designed to regulate access to the confidential personal information that is kept by the Ohio Occupational Therapy, Physical Therapy, and Athletic Trainers Board (hereinafter "Board").

(C) Application and Scope

This policy applies to all records kept by the Board, whether in electronic or paper form. Likewise, this 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.

(D) Definitions

As used in Revised Code section 1347.15 and in this 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. This includes information such as a social security number, a criminal records check result, or a disciplinary file. Simply put, if you have to redact it before releasing the information in response to a public records request, it probably is confidential personal information;

(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, any 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.

(5) "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 (e.g.: paper files) and records that are stored using electronic data processing equipment.

(E) Criteria for Access to Confidential Personal Information

R.C. 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 (including Board members) shall maintain confidentiality regarding confidential personal information acquired while employed by the Board, including, but not limited to, social security numbers of applicants/licensees, 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 Laws. Access to confidential personal information shall be granted at the lowest level necessary that allows for an individual to perform his/her assigned duties in order to minimal the potential impact to the public.

For the Board, the following criteria apply:

(1) The Executive Director and the Enforcement Division Supervisor may have unlimited access to any and all confidential personal information in the possession of the Board.

(2) The Executive Assistant may have unlimited access to any and all confidential personal information contained in the Ohio e-License System and paper files related to individuals licensed by the Board and individuals applying for licensure with the Board; any and all confidential personal information contained in criminal records checks results for individuals apply 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 of the Board.

(3) The Licensing Coordinators and Clerk may have unlimited access to any and all confidential personal information contained in the Ohio e-License System and paper files related to individuals licensed by the Board and individuals applying for licensure with the Board; and any and all confidential personal information contained in criminal records checks results for individuals apply for licensure with the Board.

(4) The Investigators may have unlimited access to any and all confidential personal information contained in disciplinary files related to alleged violations of the Board's law; any and all confidential personal information contained in the Ohio e-License System and paper files related to individuals licensed by the Board and individuals applying for licensure with the Board; and any and all confidential personal information contained in criminal records checks results for individuals apply for licensure with the Board.

(5) All Board Members may have unlimited access to any and all confidential personal information contained in the Ohio e-License System and paper files related to individuals licensed by the appropriate Section of the Board and individuals applying for licensure with the appropriate Section of the Board.

(6) The Board Members serving on an Enforcement Review Panel may have unlimited access to any and all confidential personal information contained in disciplinary files related to alleged violations of the appropriate Section's law.

(7) 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.

(8) Board employees who serve the agency in a supervisory capacity may authorize any other Board employee in their direct line of supervision or others who may be working with the Board in the course of normal business functions to have access to confidential personal information that is acquired by or in the possession of the Board. The Board organizational chart denotes those employees who serve in supervisory capacities. That organizational chart is incorporated herein by reference.

(9) Access to electronically stored data shall be granted through the use of assigned passwords that expire not less than every 180 days.

(F) Rationale for 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 reasons" are those reasons that reflect the employee's execution of the duties of the Board as set forth in Chapter 4755. of the Revised Code and in Chapters 4755-1 to 4755-48 of the 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.

(G) 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 Cty. Public Defender v. Siroki (2006), 108 Ohio St. 3d 207, 2006-Ohio-662, concerning Social Security Numbers, or the Family Educational Right to Privacy Act [FERPA], which makes confidential certain educational records*). 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 may be deemed confidential under Revised Code section 4755.02 (E), which states: "Subject to division (E)(2) of this section, information and records received or generated by the Board pursuant to an investigation are confidential, are not public records as defined in section 149.43 of the Revised Code, and are not subject to discovery in ay civil or administrative action."

(H) 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.

(I) Requests for Information from Individuals

From time to time, the Board may receive requests from individuals who want to know what confidential personal information is kept by this agency. 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.

(J) Access for Invalid Reasons

Even though appropriate safeguards are in 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 or the Director's designee 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.

(K) Data Privacy Point of Contact (DPPOC)

By law, the Board's 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.

(L) Use of Authentication Measure

Every Board employee is required to have a personal and secure password for his or her 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.

(M) 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, this policy will be copied and distributed to each Board employee for inclusion in the employee's Policy and Procedure Manual. Employees will

acknowledge receipt of the copy in writing. Amendments to this policy will be distributed and acknowledged in the same way. Further, a copy of this policy will be prominently posted in a conspicuous place in the Board office and posted on the Board website.

(N) Disciplinary Measures for Violations

No employee of the Board shall knowingly access, use, or disclose confidential personal information for reasons that would violate this policy. Knowingly accessing, using, or disclosing confidential personal information in violation of this policy is a first degree misdemeanor, is cause for immediate termination from employment, and is cause for prohibition on future employment with the State.

(O) Access to Confidential Personal Information Logs

For purposes of R.C. 1347.15 (A), the logging requirements relating to computer system "specific access by employees" do not apply when non-public information is accessed as a result of a request by an individual about that individual; or when accessing information, within an employee's scope of employment and normally assigned job duties, in order to perform research for official agency purposes, perform routing office procedures, or engage in incidental contact with the information.

Employees shall sign an attestation log to document the employee's ongoing compliance with this policy and the appropriate access and handling of confidential personal information maintained in an electronic system (log form attached). Log forms will be reviewed on a monthly basis by the Board's Data Privacy Point of Contact (Executive Director). Log forms will be maintained by the DPPOC in accordance with the Board's records retention schedule.

CONFIDENTIAL PERSONAL INFORMATION ACCESS LOG

Employee: _____

Date	Time	Name	License #/Case #	Database
1/14/11	*11:40 am*	*John Doe (sample)*	*PT.999999*	*elicense*
1/15/11	*3:15 pm*	*Jane Smith (sample)*	*OT-FY11-999*	*Discipline case log*

DPPOC Initials and Review Date: _____