

4713-1-13

**Board of cosmetology policy concerning access to confidential personal information.**

(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. Section 1347.15 of the Revised Code 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 rule is designed to regulate access to the confidential personal information that is kept by the board.

(C) Application and scope

This rule applies to all records kept by the board, whether in electronic or paper form. Likewise, this rule 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 section 1347.15 of the Revised Code and in this rule, 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 division (A)(2)(b)(5) of section 1347.12 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;
- (4) "Records" has the same meaning as set forth in division (G) of section 149.011 of the Revised Code, and

- (5) "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.

(E) Criteria for "Access to Confidential Personal Information", division (B)(1) of section 1347.15 of the Revised Code 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/licenses/[boutique services registration holders](#), and information obtained in the course of an investigation, including client 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 minimize the potential impact to the public. For the board, the following criteria apply:

- (1) The executive director and the managers as selected by the executive director may have unlimited access to any and all confidential personal information in the possession of the board;
- (2) The executive director may delegate to the staff involved with administrative violations unlimited access to any and all confidential personal information contained in the Ohio official licensing 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 applying for licensure [or boutique services registration](#) with the board;
- (3) The staff members working on granting licenses, [boutique services registrations](#), or permits and renewing licenses, [boutique services registrations](#), or permits may have unlimited access to any and all confidential personal information contained in the Ohio official licensing system and paper files related to individuals licensed [or issued boutique services registrations](#) by the board and individuals applying for licensure [or boutique services registration](#) with the board; and any and all confidential personal information contained in criminal records checks results for individuals applying for licensure [or boutique services registration](#) with the board including test results;
- (4) The investigators, inspectors and compliance coordinator 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 official licensing system and paper files related to individuals licensed [or issued boutique services registrations](#) by the board and individuals applying for licensure [or boutique services registration](#) with the board, and any and all confidential personal information contained in criminal records checks results for individuals who apply for licensure [or boutique services registration](#) with the board. In addition, the compliance coordinator may have unlimited access to confidential test questions and test procedures as well as test results;

- (5) The business manager and office manager may have access to all personnel records of the board and all financial records contained on paper or in OAKS or "My Ohio";
- (6) The examination and testing staff may have unlimited access to any and all confidential personal information contained in the Ohio official licensing system and paper files related to individuals licensed [or issued boutique services registrations](#) by the board and individuals that are part of a continuing education or testing process;
- (7) The board members serving on a personnel committee may have unlimited access to any and all confidential personal information contained in disciplinary files related to alleged violations of the appropriate law or rule;
- (8) All board employees are entitled to access their own OAKS or "My Ohio" information and all other confidential personal information kept on file for payroll and other time and hour functions;
- (9) 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, and
- (10) The board's assistant attorney general or any attorney or attorneys assigned by the attorney general to the board may have access to any files necessary to prepare for a hearing or to provide the board with a requested informal legal opinion.

- (11) Access to electronically stored data shall be granted through the use of assigned passwords.
- (F) The following systems contain confidential personal information held by the board:
- (1) The Ohio official licensing system contains social security numbers and investigative information, and
  - (2) The electronic document management system contains social security numbers on documents including applications, supporting documents and investigative files.
- (G) 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 reasons” are those reasons that reflect the employee’s execution of the duties of the board as set forth in Chapter 4713. of the Revised Code and in Chapters 4713-1 to 4713-21 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.
- (H) Statutory and other legal authority for confidentiality. The term “confidential personal information” is defined by sections 1347.15 and 149.43 of the Revised Code. 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). 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 section 4713.24 of the Revised Code, which makes confidential the questions for and results of the licensing examination.
- The Ohio supreme court has held that although the federal Privacy Act (5 U.S.C 552a) does not expressly prohibit release of one’s SSN, the act does create an expectation of privacy as to the use and disclosure of the SSN.
- (I) 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.

(J) 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. Board employees receiving such a request shall consult with the executive director before any response is provided.

(K) Access for invalid reasons. Even though there are appropriate safeguards 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.

(L) 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 section 1347.15 of the Revised Code 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.

(M) 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.

(N) 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 rule will be distributed and acknowledged in the same way. Further, a copy of this rule will be prominently posted in a conspicuous place in the board office and posted on the board website.

(O) Disciplinary measures for violations

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