OHIO RESPIRATORY CARE BOARD

POLICY # 2.95 (b)

SUBJECT: Accessing Non-Public Personal Information Policy

Effective Date: 10-13-2010
Replaces Policy #2.95a effective 2-10-2009
Prior effective date: 2-10-2009
6-9-2009

Administrative Approval: _____
President

_____
Executive Director

Authority: This policy is issued in compliance with Ohio Administrative Code 4761-2-02, which authorizes the Executive Director of the Ohio Respiratory Care Board (ORCB) to act as the chief administrative officer of the Board and manage the staff and board resources as required to meet the obligations, goals and objectives of the agency; and pursuant to the Governor's November 20, 2008 Management Directive (Revised), "Accessing Sensitive Personal Information Maintained by the State"; and pursuant to Section 1347.15, Ohio Revised Code (ORC) and rules adopted thereunder.

Purpose: The purpose of this policy is to provide employees with the knowledge necessary to properly access and protect confidential and sensitive personal information collected and maintained by the ORCB under the authority found in Chapters 4761 and 4752 of the Revised Code, as well as any other state or federal regulations that require the Board to collect and maintain such information. The policy includes a framework for granting and reviewing access rights to records that contain confidential and sensitive personal information.

Applicability: All ORCB Employees.

Definitions:

1. "Non-public Personal Information" – means non-public personal information that describes anything about a person; that indicates actions done by or to a person; that indicates a person possesses certain personal characteristics; that contains information, and can be retrieved from a "system" by a name, symbol or other identifying number assigned to a person; and/or carries a higher risk to the subjects of the information, if such information is misused or placed in the wrong hands. Non-public personal information may include data related to an individual's educational,

financial, health/medical, criminal or employment history; social security numbers; federal tax identification numbers or financial account numbers.

For purposes of this policy, it is intended that the term "Non-Public Personal Information" includes "Sensitive Personal Information" as defined in the Governor's November 20, 2008 Management Directive, and "Confidential Personal Information" – personal information that is not a public record for purposes of Section 149.43, ORC, as defined in Section 1347.15(A), ORC.

2. "System" – for the purpose of this policy 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 and records that are stored using electronic data processing equipment. "System" does not include collected archival records in the custody of or administered under the authority of the Ohio historical society, published directories, reference materials or newsletters, or routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person.

3. Non-public personal Information – can exist in electronic and/or paper format including but not limited to paper applications and application material, reports or screen shots generated from a computerized system that contains non-public personal information. Non-Public Personal Information cannot be transmitted verbally, electronically, visually, or in a written or other tangible form to unauthorized person.

4. Non-public information may be found in a system (as defined above) or in non-system records, such as correspondence and memorandums received by or generated by the ORCB.

5. In accordance with Section 1347.04(A)(1)(e)of the Revised Code, "personal information," including non-public personal information, does not include, personal information systems that are comprised of investigatory material compiled for law enforcement purposes by the ORCB.

6. User Access Classifications – for the purpose of this policy refer to users or groups of users who access common record sets or systems to perform their assigned duties.

Policy: It is the policy of the ORCB 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 ORCB. Legitimate governmental objectives of the ORCB include those functions set forth in Chapters 4761 and 4752 of the Revised Code and Administrative Rules adopted there under, and administrative support functions necessary to further those objectives, including but not limited to: investigation of information related to violations of Chapters 4761 and 4752 of the Revised Code ORC, or rules adopted by the ORCB; adjudication of disciplinary actions;

monitoring the compliance of individuals under consent agreement; or processing initial applications for, or renewal of, limited permits/certification/licensure.

Procedures:

1. ORCB employees shall maintain confidentiality regarding non-public personal information acquired while employed by the Board, including but not limited to social security numbers of applicants/limited permit holders/licensee/certificate holders and Board employees, applicant/limited permit/licensee/certificate holder investigative records (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.

2. Access to non-public personal information shall be granted at the lowest level necessary that allows an individual to perform their assigned duties in order to minimize the potential impact to the public. Each job position in the agency shall be evaluated and assigned an access classification based upon the specific and legitimate duties of the position as it relates to the official governmental objectives of the ORCB.

   a. The Executive Director shall serve as the ORCB's Data Privacy Point of Contact (DPPOC).

   b. The DPPOC shall determine the level of access for each of the ORCB's position.

   c. Access to electronically stored data shall be granted using assigned passwords that expire after not more than 180 days. Employees are responsible for maintaining the security and use of their usernames and passwords for all data systems maintained by the ORCB.

   d. Extensive increases in an individual's or user classification's access to non-public personal information will be evaluated by the DPPOC.

   e. Individually assigned user access classifications shall be re-evaluated no less than annually.

3. **User Classification Assignment:** Employees will be assigned to one or more user classifications based on their duties and the known systems or information they access to perform their legitimate assigned duties. Access to each system is granted on an as-needed basis and is not automatically granted by virtue of inclusion in a group.

   i. Executive Director – General Access and Administrative Access Class I.
   ii. Administrative Assistant III - General Access and Administrative Access Class II.
   iii. License Certification Examiner II – General Access and Licensure/Certification

Access.

iv. Investigator – General Access and Investigation/Compliance Access
v. Board Members – Access assigned as needed by Executive Director.

4. **User Classifications:**

a. General Access Class: Some records are collected and maintained by the ORCB, but are not, by definition, maintained in a "system." This material will hold the access classification as "general access." General access records are normally public records, but could contain Non-public Personal Information and must always be reviewed to determine if redaction of confidential/sensitive information is necessary before releasing the record or printing the record/copying the record for internal use.

In the course of working at the ORCB, staff may inadvertently receive Non-Public Personal Information that is not part of their normal job duties. If this happens, staff shall protect the security of this information give it to their reporting supervisor. Reporting supervisor's shall determine how best to handle the information, which may include confidentially returning the information to the sender.

General Access is granted to the following:

i. Vendor records (paper): includes invoices, vouchers and proof of payments;
ii. Incoming and outgoing correspondence, excluding confidential correspondence, such as legal and investigative correspondence;
iii. Memorandums, excluding internal personnel memorandums and legal memorandums;
iv. Meeting minutes and journal entries;
v. Emails, excluding confidential emails, such as legal and investigative emails;
vi. Forms and applications, including brochures and instructional pamphlets;
vii. Fiscal records (paper);
viii. Law and rules; and
ix. Policies and Procedures, excluding non-public policies.

b. Licensure/Certification Access Class: user(s) may be granted access to the following for purposes of creating or modifying applicant/limited permit/licensee/certificate holder records, reviewing applicants for licensure/certification and responding to public inquiries regarding the same:

i. Mail: includes licensure verification requests, transcripts, BCI&I/FBI reports, for the purpose of processing and routing;
ii. eLicensing Database;
iii. BCI&I / FBI paper records;

iv. Paper and/or electronic (Scanned) copies of applications that include social security numbers and documents, including but not limited to educational transcripts, verification of education forms, credential verification reports , and employee lists;
v. Health Integrity and Protection Database (HIPDB) (external source) for data entry only;
vi. Disciplinary Action routing forms;
vii. National Board for Respiratory Care, Inc. (NBRC) examination report, credential verification reports, credential lists that contain redacted or full social security numbers; and
viii. Paper and/or electronic (Scanned) copies of renewal, reactivation and reinstatement applications that include social security numbers and documents, including but not limited to continuing education documents.

c. **Investigation/Compliance Access Class:** user(s) may be granted access to the following for purposes of investigating information regarding violations of the Respiratory Care and Home Medical Equipment Practice Acts or rules adopted by the ORCB; adjudication of disciplinary actions; monitoring the compliance of individuals under consent agreement and/or under the terms of alternative to discipline monitoring programs; and reporting disciplinary actions as required by federal and/or state law and law enforcement purposes:

i. Health Integrity and Protection Database (HIPDB) (external source);
ii. BCI&I / FBI Paper Reports (external source);
iii. Investigation, Proposed Board Action, and Post-Disciplinary Monitoring Databases (internal);
iv. FirstLab Database (external source);
v. ELicensing Database;
vi. Paper and/or electronic investigative files, post-disciplinary monitoring files, alternative to discipline monitoring program files, that include social security numbers and investigative records, including but not limited to patient records, alcohol/drug screens reports, employer reports, witness statements, prescription reports, examination reports and assessments and/or educational records;
vii. Paper and/or electronic (Scanned) copies of applications that include social security numbers and documents, including but not limited to educational transcripts, verification of education forms, credential verification reports , and employee lists; and
viii. Paper and/or electronic (Scanned) copies of renewal, reactivation and reinstatement applications that include social security numbers and documents, including but not limited to continuing education documents; and
ix. Disciplinary Action routing forms.

d. **Administrative I Access Class:** user(s) may be granted access to the following:

i. Health Integrity and Protection Database (HIPDB) (external source);
ii. BCI&I / FBI Paper Reports (external source);
iii. Investigation, Proposed Board Action, and Post-Disciplinary Monitoring Databases (internal);
iv. ELicensing Database: to perform license/certification approvals, license verifications, validate and verify administrative actions records, perform quality assurance reviews, and revenue and financial transactions and reporting related to applicant and credential processing and deposits;
v. Paper and/or electronic investigative files, post-disciplinary monitoring files, alternative to discipline monitoring program files, that include social security numbers and investigative records, including but not limited to patient records, alcohol/drug screens reports, employer reports, witness statements, prescription reports, examination reports and assessments and/or educational records.
vi. Paper and/or electronic (Scanned) copies of applications that include social security numbers and documents, including but not limited to educational transcripts, verification of education forms, credential verification reports, and employee lists;
vii. Paper and/or electronic (Scanned) copies of renewal, reactivation and reinstatement applications that include social security numbers and documents, including but not limited to continuing education documents.
viii. Disciplinary Action routing forms;
ix. Legacy Standard Renewal System Records (electronic);
x. Miscellaneous data files (temporary);
xi. National Board for Respiratory Care, Inc. (NBRC) examination report, credential verification reports, credential lists that contain redacted or full social security numbers;
xii. Personnel records (internal);
xiii. Position applications (internal);
xiv. OAKS Human Capital Management (HCM) for the purpose of processing payroll and other Human Resources functions as the primary (or backup);
xv. OAKS Financials for the purpose of processing revenue and payables as the primary (or backup); and
xvi. Administrative access to external and internal data sources, in order to create user accounts and establish/modify access rights

e. **Administrative II Access Class:** user(s) may be granted access to the following:

i. ELicensing Database: to validate and verify administrative actions records, perform quality assurance reviews, and revenue and financial transactions and reporting related to applicant and credential processing and deposits;
ii. Paper and/or electronic (Scanned) copies of applications that include social security numbers and documents, including but not limited to

educational transcripts, verification of education forms, credential verification reports, and employee lists;

iii. Personnel records for assigned employees (internal);

iv. OAKS Human Capital Management (HCM) for the purpose of processing payroll and other Human Resources functions as the primary (or backup);

v. OAKS Financials for the purpose of processing revenue and payables as the backup;

vi. Administrative access to external and internal data sources, in order to create user accounts and establish/modify access rights; and

vii. Paper and/or electronic (Scanned) copies of renewal, reactivation and reinstatement applications that include social security numbers and documents, including but not limited to continuing education documents.

5. **Logging access to Non-Public Personal Information:**

For purposes of Section 1347.15(A), ORC, the logging requirements of that Section 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 routine office procedures, or engage in incidental contact with the information.

a. Employees shall complete a Specific Access Log (**Specific Access Log form attached**) each time a computer system is "specifically accessed." This log must be completed each time non-public information is accessed: (i) **not** at the result of a request by an individual about that individual; and the access is (ii) **not** within an employee's scope of employment or **not** within the employee's normally assigned job duties.

b. Employees shall transmit electronically or manually any Specific Access Logs to the DPPOC. The DPPOC shall retain a copy of these records in accordance with the records retention schedule.

6. **Public Records Requests:**

Employees shall carefully review all information released when complying with public records requests to ensure that non-public personal information is not included in the response. The DPPOC (Executive Director) will review all public records requests prior to release of information.

7. **Handling, Storing, and Transmitting:**

Employees shall handle, store and transmit non-public personal information in a secure method approved by the ORCB.

8. **Records Retention:**
Employees shall dispose of non-public personal information in a secure method approved by the ORCB and in compliance with the ORCB's records retention schedules or the State's general records retention schedules.

a. Optical Disks (CDs, DVDs), shall be shredded in the office prior to disposal in accordance with policies and procedures established by the Board for those documents.

b. BCI&I documents, database reports and paper material shall be shredded utilizing the secured shredding bins provided.

c. Electronic Storage Media (ie. tapes, drives, portable storage devices) shall be reformatted using an approved multi-pass over-write process if being reused or destroyed through Tech-Disposal prior to disposal or salvage.

9. **Requests for Records by Individuals:**

The ORCB will comply with any written request from an individual for a list of Non-Public Personal Information that the ORCB keeps on that individual, unless the Non-Personal Information relates to an investigation about the individual based on specific statutory authority. The Executive Director will review all such requests.

10. **Improper Access:**

In the event an employee of the ORCB improperly accesses an individual's non-public sensitive information, the ORCB shall inform the individual in writing within 15 days of determination of such access.

11. **Policy Review:**

This policy and the User Classifications/Access shall be reviewed annually.

12. **Disciplinary Action:**

Suspected or observed improper access should be reported to the DPPOC (Executive Director). If an employee suspects or observes inappropriate access by a manager, the employee shall report the access to the Board President. Employees of the board who inappropriately access sensitive information for impermissible purposes are subject to disciplinary action as set forth in the ORCB policies 2.6 and 2.7, including termination and/or legal action.

Forms: Specific Access Log