Ohio Board of Nursing www.nursing.ohio.gov
17 S. High Street, Suite 660 • Columbus, Ohio 43215-3466 • 614-466-3947

Subject: Personal Information Systems	Page 1 of 6
Policy Number: S-OPS-014	
Approved:	Effective Date: February 5, 2018

Authority: This policy is issued in compliance with Ohio Revised Code 4723.05, which authorizes the Executive Director of the Ohio Board of Nursing (OBN) to establish standards for the conduct of employees and to act as the chief administrative officer of the OBN; pursuant to the Governor's November 20, 2008 Management Directive, "Accessing Sensitive Personal Information Maintained by the State;" and pursuant to Chapter 1347, Ohio Revised Code (ORC), and rules adopted thereunder.

Purpose: The purpose of this policy is to provide employees with the knowledge necessary for properly accessing and handling personal information within systems maintained by the OBN. The policy includes a framework for granting and reviewing access rights to confidential personal information.

Applicability: All OBN Employees.

Definitions:

1. Data Privacy Point of Contact (DPPOC) – the DPPOC is an employee designated by the Executive Director to work with the chief privacy officer within the State Office of Information Technology to ensure that Confidential Personal Information (CPI) is protected and employees comply with Chapter 1347, ORC, the rules adopted under that Chapter, and this policy.

2. Personal Information; Confidential Personal Information - personal information means information that describes anything about a natural person; that indicates actions done by or to a person; that indicates a person possesses certain personal characteristics; that can be retrieved from a "system" by a name, identifying number, symbol, or other identifier assigned to a person. Confidential Personal Information means personal information that is not a public record for purposes of Section 149.43, ORC. For purposes of this policy, it is intended that CPI includes "Sensitive Personal Information" as defined in the Governor's November 20, 2008 Management Directive.

3. System – for the purpose of this policy refers to any collection or group of related records that the OBN maintains, meaning any record the OBN owns, has control over, or responsibility or accountability for, including but not limited to electronic or paper files and databases.

4. User Access Classifications – for the purpose of this policy refer to users or groups of users who access common data sets or systems to perform their assigned duties. The DPPOC shall maintain the User Access Classification information.

Policy: It is the policy of the OBN to restrict access to CPI to only those employees who need access to perform a specific, legitimate governmental objective on behalf of the OBN. Legitimate governmental objectives of the OBN include those functions set forth in Chapter 4723, ORC, and Rule 4723-1-09, Ohio Administrative Code (OAC), and include administrative support functions necessary to further those objectives, including but not limited to: investigation of information related to violations of Chapter 4723, ORC, or rules adopted by the OBN; adjudication of disciplinary actions; monitoring the compliance of individuals under consent agreement and/or under the terms of alternative to discipline monitoring programs; processing initial applications for, or renewal of, certification/licensure; survey, review and/or approval of pre-licensure nursing education and training programs.

Procedures:

1. OBN employees shall maintain confidentiality of CPI acquired while employed by the OBN, including but not limited to social security numbers of applicant/licensee/certificate holders and OBN employees, applicant/licensee/certificate holder investigative, monitoring and alternative to discipline program information (including patient records contained in investigative files). Confidentiality must be maintained both during and after employment with the OBN as required by Ohio Ethics Law, and in accordance with Standards of Ethical Conduct, S-OPS-008.

2. Access to CPI 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.

    a. Managers shall work closely with the DPPOC to determine the necessary level of access.

    b. Access to electronically stored data shall be granted through the use of assigned passwords that expire after not more than 180 days.

    c. Extensive increases in an individual's or user classification's access to CPI will be evaluated by the DPPOC and approved by the Executive Director.

    d. Individually assigned user access classifications shall be re-evaluated no less than annually. Employees moving from one position to another with the OBN will be re-evaluated based on their newly assigned job duties.

3. 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 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.

    a. General Access Class: user(s) may be granted access to the following:
        i. The primary licensure database (eLicensing) for the purpose of handling general inquiries and routing program specific callers;
        ii. Mail which includes BCI&I reports, for the purpose of processing and routing.

b. Licensure/Certification Access Class: user(s) may be granted access to the following for purposes of creating or modifying applicant/licensee/certificate holder records, approving applicants for licensure/certification and responding to public inquiries regarding the same:
   i. eLicensing Database;
   ii. BCI&I Database (internally maintained / external source) and paper records;
   iii. PearsonVue NCLEX Exam Database (external source);
   iv. Nursys Database (external source);
   v. HeadMaster Database (external source);
   vi. Systematic Alien Verification & Entitlements (SAVE) Database (external source);
   vii. Paper and/or electronic copies of applications that include social security numbers and documents, including but not limited to educational transcripts.

c. Renewal Access Class: user(s) may be granted access to the following for purposes of maintaining, reactivating, reinstating, and/or auditing existing licensee/certificate holder records, approving applicants for renewal and responding to public inquiries regarding the same:
   i. eLicensing Database;
   ii. Nursys Database (external source);
   iii. Paper and/or electronic copies of renewal, reactivation and reinstatement applications that include social security numbers and documents, including but not limited to continuing education documents.

d. Compliance Access Class: user(s) may be granted access to the following for purposes of investigating information regarding violations of the Nurse Practice Act or rules adopted by the OBN; 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. Fraud Imposter Tracking System (FITS) (external source);
   ii. Health Integrity and Protection Database (HIPDB) (external source);
   iii. BCI&I Paper Reports (external source);
   iv. Investigation, Proposed Board Action, and Post-Disciplinary Monitoring Databases (internal);
   v. Alternative to Discipline Program Databases;
   vi. National Council State Board of Nursing -Nursys (external source);
   vii. FirstLab Database (external source);
   viii. eLicensing Database;
   ix. Paper and/or electronic investigative files, post-disciplinary monitoring files, alternative to discipline monitoring program files, that include social security numbers and records, including but not limited to patient records, alcohol/drug screens reports, employer reports, prescription reports, examination reports and assessments and/or educational records.

e. Administrative Access Class I: user(s) may be granted access to the following:
   i. OAKS Human Capital Management (HCM) for the purpose of processing payroll and other Human Resources functions as the primary (or backup);
   ii. OAKS Financials for the purpose of processing revenue and payables as the primary (or backup);
   iii. eLicensing database to perform financial transactions and reporting related to applicant and credential processing.

f. Administrative Access Class II: user(s) may be granted access to the following: Administrative access to external data sources, in order to create user accounts and establish/modify access rights (i.e., eLicensing, NCSBN, Nursys, FITS, PearsonVue, SAVE, etc.)

g. Administrative Access Class III: user(s) may be granted access to the following: Administrative access to internal systems in order to create user accounts and establish/modify access rights.

4. Regarding records stored in electronic databases that the OBN maintains (i.e., databases the OBN owns, has control over, or responsibility or accountability for), that do not have a mechanism for recording specific access by employees to CPI, then employees shall do the following:

a. On a daily basis, employees shall maintain a log that documents their access of CPI contained in electronic record systems. Log forms will be provided to each employee by their supervisor or the DPPOC, based upon the employee's assigned work responsibilities and user classification.

b. All logs shall document the name of the person whose CPI was accessed, the date, and the electronic system(s) accessed with respect to that person. The employee shall sign the log at the end of each month attesting that each access of CPI was for valid reasons related to the employee's job duties, or the OBN's government function, as set forth in Section 1347.15(B)(2), ORC, and Rule 4723-1-09, OAC, and submit the log to the DPPOC.

c. Logging shall not be required in the following situations:

   i. The person who is the subject of the CPI requested that the OBN or employee take some action on the person's behalf and accessing the CPI is required in order to consider or process the request. *Examples include, but are not limited to, the following*:
      a) The person is an applicant for licensure/certification or renewal, and the employee accesses CPI to process an application;
      b) The person is a licensee/certificate holder, and the employee accesses CPI to respond to a public request to confirm the person's license/certificate status;

c) The person is being monitored by the Board according to the terms of a Consent Agreement or alternative to discipline agreement, and the employee accesses CPI in order to review, monitor and document the person's compliance with the agreed-upon terms and conditions.

ii. The person requests their own CPI;

iii. CPI is accessed in order to run a report, conduct research or perform routine office functions not specifically directed toward any one person;

iv. An employee comes into incidental contact with CPI and the access is not specifically directed toward a named person or group of persons.

d. The DPPOC shall maintain employee logs according to the OBN's records retention schedule, ADM-04.

5. Invalid Access of CPI. Upon discovery that an employee has accessed CPI for an invalid reason, the incident shall be investigated by the employee's manager in consultation with the DPPOC and Chief Legal Counsel, as necessary, and the person whose CPI was improperly accessed shall be notified as required by Rule 4723-1-08, OAC. An incident report shall be prepared in accordance with Incident Reporting, S-OPS-001.

6. Employees shall carefully review all information released when complying with public records requests to ensure that CPI is not included in the response.

7. Requests by persons for lists of CPI about the person shall be handled by the DPPOC in a manner that complies with Rule 4723-1-08 (B), OAC.

8. Employees shall handle, store and transmit CPI in a secure method approved by the OBN.

9. Employees shall dispose of CPI in a secure method approved by the OBN.

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

b. 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 prior to disposal or salvage.

d. IT equipment and computer media that is to be permanently transferred shall have all information overwritten with meaningless data in such a way that information cannot be reasonably recovered. For sensitive or personally identifiable information, as the

levels of confidentiality and risk merit, IT personnel shall increase the number of overwrites or physically destroy the IT equipment to ensure that information cannot be recovered.

e. IT equipment may only be sent to IT sanitation service providers who have agreed in writing to:

   i. Maintain the confidentiality of state information;
   ii. Access information only if it is necessary for sanitation purposes; and
   iii. Sanitize any equipment or components capable of storing information in accordance with state and Board of Nursing policy.

10. On an annual or more frequent basis, as needed, employees shall attend a training session regarding this policy and applicable law and rules related to access to CPI. Employees shall sign a receipt acknowledging their receipt of this Policy.
11. Failure to comply with this and any other OBN policies relating to the access and handling of CPI is prohibited, and may result in discipline as set forth in the Standards of Employee Conduct, S-HR-001.

12. This policy is in addition to the requirements imposed by Rules 4723-1-07 to 4723-1-11, OAC, for personal information systems.

13. A copy of this policy shall be posted in the public lobby of the OBN office and posted on the OBN's website.

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

Forms: Unit specific logs will be provided to each employee by his/her supervisor.