3901-1-02 **Access to confidential personal information.**

(A) Purpose

~~This~~ The purpose of this rule is to ~~regulate~~ standardize employee access to the confidential personal information that the department of insurance (department) keeps. This rule applies to both electronic records and records kept on paper.

(B) Authority

This rule is promulgated ~~under the authority of~~ pursuant to the authority vested in the superintendent under section 3901.041 of the Revised Code and division (B) of section 1347.15 of the Revised Code that requires each state agency to adopt rules under Chapter 119. of the Revised Code to ~~regulate~~ standardize access to confidential personal information. ~~Section 3901.041 of the Revised Code provides that the superintendent of insurance (superintendent) shall adopt, amend and rescind rules to discharge the superintendent's duties and exercise the superintendent's powers.~~

(C) Definitions

For the purpose of this rule promulgated in accordance with section 1347.15 of the Revised Code, the following definitions, as set out by the department of administrative services in rule 123:3-2-01 of the Administrative Code, apply:

(1) "Access" as a noun means an instance of copying, viewing, or otherwise perceiving whereas "access" as a verb means to copy, view, or otherwise perceive.

(2) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as of the effective date of the agency rule addressing requirements in section 1347.15 of the Revised Code.

(3) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, or retrieves personal information using electronic data processing equipment.

(4) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the agency in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the agency

confidential.

(5) "Employee of the state agency" means each employee of a state agency regardless of whether he or she holds an elected or appointed office or position within the state agency. "Employee of the state agency" is limited to the specific employing state agency.

(6) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.

(7) "Individual" means a natural person or the natural person's authorized representative, legal counsel, legal custodian, or legal guardian.

(8) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.

(9) "Person" means a natural person.

(10) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

(11) "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code. "System" includes manual and computer systems.

(12) "Research" means a methodical investigation into a subject.

(13) "Routine" means commonplace, regular, habitual, or ordinary.

(14) "Routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person" as that phrase is used in division (F) of section 1347.01 of the Revised Code means personal information relating to employees and maintained by the agency for internal administrative and human resource purposes.

(15) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

(16) "Upgrade" means a substantial redesign of an existing computer system for the

purpose of providing a substantial amount of new application functionality, or application modifications that would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements.

(D) Procedures for accessing confidential personal information (as required by divisions (B)(1) and (B)(5) to (B)(8) of section 1347.15 of the Revised Code).

For personal information systems, whether manual or computer systems, which contain confidential personal information, the department shall do the following:

(1) Criteria for accessing confidential personal information

Personal information systems of the department are managed on a "need-to-know" basis whereby the information owner determines the level of access required for an employee of the department to fulfill his or her job duties. The determination of access to confidential personal information shall be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The department shall establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer require access to confidential personal information in a personal information system, the employee's access to confidential personal information shall be removed.

(2) Individual's request for a list of confidential personal information

Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the department, the department shall do all of the following:

(a) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information;

(b) Provide to the individual the list of confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and

(c) If all information relates to an investigation about that individual, inform

the individual that the agency has no confidential personal information about the individual that is responsive to the individual's request.

(3) Notice of invalid access

(a) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the department shall notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. However, the department shall delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the department may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system.

"Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once the department determines that notification would not delay or impede an investigation, the department shall disclose the access to confidential personal information made for an invalid reason to the person.

(b) Notification provided by the department shall inform the person of the type of confidential personal information accessed and the date(s) of the invalid access.

(c) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic or telephone notice.

(4) Appointment of a data privacy point of contact

The superintendent shall designate an employee of the department to serve as the data privacy point of contact. The data privacy point of contact shall work with the chief privacy officer within the office of information technology to assist the department with both the implementation of privacy protections for the confidential personal information that the department maintains and compliance with section 1347.15 of the Revised Code and the rules adopted pursuant to the authority provided by that chapter.

(5) Completion of a privacy impact assessment

The superintendent shall designate an employee of the department to serve as the data privacy point of contact who shall timely complete the privacy impact assessment form developed by the office of information technology.

(E) Valid reasons for accessing confidential personal information ~~(as required by division (B)(2) of section 1347.15 of the Revised Code)~~

Pursuant to the requirements of division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the department's exercise of its powers or duties, for which only employees of the department may access confidential personal information regardless of whether the personal information system is a manual system or computer system.

Performing the following functions constitute valid reasons for authorized employees of the department to access confidential personal information:

(1) Responding to a public records request;

(2) Responding to a request from an individual for the list of confidential personal information the department maintains on that individual;

(3) Administering a constitutional provision or duty;

(4) Administering a statutory provision or duty;

(5) Administering an administrative rule provision or duty;

(6) Complying with any state or federal program requirements;

(7) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;

(8) Auditing purposes;

(9) Licensure processes;

(10) Investigation or law enforcement purposes;

(11) Administrative hearings;

(12) Litigation, complying with an order of the court, or subpoena;

(13) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary and compensation issues, leave requests and issues, time card approvals and issues);

(14) Complying with an executive order or policy;

(15) Complying with a department policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency; or

(16) Complying with a collective bargaining agreement provision.

(F) Confidentiality statutes (as required by division (B)(3) of section 1347.15 of the Revised Code)

The following federal statutes or regulations or state statutes and administrative rules make personal information maintained by the department confidential and identify the confidential personal information within the scope of rules promulgated by the department in accordance with section 1347.15 of the Revised Code:

(1) Social security numbers: 5 U.S.C. section 552a; division (A) of section 149.45 of the Revised Code; "State ex rel. Beacon Journal Publishing Co. v. City of Akron, 70 Ohio St.3d 605 (1994)."

(2) Consumer credit reporting information: limits the use that can be made of consumer credit reports: 15 U.S.C. section 1681b.

(3) Federal tax returns and return information: 26 U.S.C. section 6103(a).

(4) Medical records pertaining to an eligible person under the American with Disabilities Act: 42 U.S.C. section 12112(d)(3)(B).

(5) Bureau of criminal identification and investigation records: division (H) of section 109.57 of the Revised Code and section 4776.04 of the Revised Code.

(6) Public employees retirement system (PERS) information (the individual's

statement of previous service, amount of a monthly allowance or benefit paid to an individual and the individual's personal history record that includes address, telephone number, social security number, record of contributions, correspondence with the public employees retirement system or other information determined by the public employees retirement board to be confidential): division (A) of section 145.27 of the Revised Code.

(7) Medical reports and recommendations required by the public employees retirement system: division (B) of section 145.27 of the Revised Code.

(8) Deferred compensation program participant information: divisions (A) and (B) of section 148.05 of the Revised Code.

(9) Medical records: division (A)(1)(a) of section 149.43 of the Revised Code.

(10) Confidential law enforcement investigatory records: division (A)(1)(h) of section 149.43 of the Revised Code.

(11) Security and infrastructure records: section 149.433 of the Revised Code.

(12) Health insuring corporation complaint and response documents and information that contain medical records provided to the superintendent: division (C) of section 1751.19 of the Revised Code.

(13) Any data or information pertaining to the diagnosis, treatment, or health of any enrollee or applicant for enrollment that is obtained by the health insuring corporation from the enrollee or applicant, or from any health care facility or provider: division (B) of section 1751.52 of the Revised Code.

(14) Peer review committee records: sections 1751.21 and 2305.252 of the Revised Code.

(15) Medical records; doctor patient communications: division (B) of section 2317.02 of the Revised Code; "TBC Westlake, Inc. v. Hamilton Cty. Bd. of Revision, 81 Ohio St.3d 58, 62 (1998)."

(16) Identity of an individual on whom an HIV test is performed, the results of the test and the identity of any individual diagnosed as having AIDS or an AIDS-related condition: section 3701.243 of the Revised Code.

(17) Records pertaining to an insurance fraud investigation are confidential law enforcement investigatory records (CLEIR) and are protected to the extent of the CLEIR exemption from section 149.43 of the Revised Code until the expiration of all applicable federal and state statutes of limitation: section 3901.44 of the Revised Code.

(18) Applicant HIV test results required by insurers when underwriting fraternal policies: section 3901.46 of the Revised Code.

(19) Records and information pertaining to an investigation of a license applicant or of an agent, solicitor, broker or a person licensed under the code sections covering public insurance adjusters and third party administrators until notice and opportunity for hearing is given or until three years have passed since the close of the investigation: section 3905.24 of the Revised Code.

(20) All medical information solicited or obtained by any viatical settlement licensee: division (G) of section 3916.07 of the Revised Code.

(21) Names and individual identification data for all viators: division (D)(1) of section 3916.11 of the Revised Code.

(22) All proprietary information of a viatical settlement licensee, all individual transaction data regarding the business of viatical settlements and data that could compromise the privacy of personal, financial and health information of the viator or insured: division (E) of section 3916.12 of the Revised Code.

(23) With certain specified exceptions, identity as a viator or a viatical settlement insured, including the viator's or the insured's name and individual identification data, or the viator or the insured's financial or medical information: section 3916.13 of the Revised Code.

(24) Documents and evidence provided to or obtained by the superintendent in an investigation of any suspected or actual fraudulent viatical settlement acts or fraudulent insurance acts: division (E)(1) of section 3916.18 of the Revised Code.

(25) Records containing information pertaining to the medical history, diagnosis, prognosis or medical condition of a covered person pursuant to the external review laws under Chapter 3922. of the Revised Code and sections 1751.77 to 1751.87 of the Revised Code: section 3922.21 of the Revised Code.

(26) Medical claims data required to be reported to the superintendent ~~by section 3929.302 of the Revised Code~~: division (G) of section 3929.302 of the Revised Code.

(27) Driver's license number or state identification card number: section 4501.27 of the Revised Code and 18 U.S.C. sections 2721 and 2725.

(28) Law enforcement automated data system (LEADS) information: section 5503.10 of the Revised Code and rule ~~4501:2-10-06~~ 4501:2-10-03 of the Administrative Code.

(29) Any information gained as the result of returns, investigations, hearings, or verifications required or authorized by Chapter 5747. of the Revised Code on income tax: section 5747.18 of the Revised Code.

(30) Personal information: division (A)(1)(dd) of section 149.43 of the Revised Code, based on the definitions in division (A)(1) of section 149.45 of the Revised Code.

(31) Records and documents relating to certifications, recertifications or medical histories of employees' family members, created for purposes of the Family and Medical Leave Act: 29 C.F.R. section 825.500(g).

As statutes are enacted or amended and rules are promulgated or revised, the list of confidentiality provisions provided in this rule may be subject to change. Any changes that occur before the time of the five-year rule review process for this rule shall be available to any requester by making a request to the department's office of legal services.

(G) Restricting and logging access to confidential personal information in computerized personal information systems (as required by divisions (B)(4) and (B)(9) of section 1347.15 of the Revised Code)

For personal information systems that are computer systems and contain confidential personal information, the department shall do the following:

(1) Access restrictions

Access to confidential personal information that is kept electronically shall require a password or other authentication measure.

(2) Acquisition of a new computer system

When the department acquires a new computer system that stores, manages or contains confidential personal information, the department shall include a mechanism for recording specific access by employees of the department to confidential personal information in the system.

(3) Upgrading existing computer systems

When the department modifies an existing computer system that stores, manages or contains confidential personal information, the department shall make a determination whether the modification constitutes an upgrade. Any upgrades to a computer system shall include a mechanism for recording specific access by employees of the department to confidential personal information in the system.

(4) Logging requirements regarding confidential personal information in existing computer systems

(a) The department shall require employees of the department who access confidential personal information within computer systems to maintain a log that records that access.

(b) Access to confidential personal information is not required to be entered into the log under the following circumstances:

(i) The employee of the department is accessing confidential personal information for official department purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(ii) The employee of the department is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iii) The employee of the department comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iv) The employee of the department accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(a) The individual requests confidential personal information about himself or herself.

(b) The individual makes a request that the department takes some action on that individual's behalf and accessing the confidential personal information is required in order to consider or process that request.

(c) For purposes of this paragraph, the department may choose the form or forms of logging, whether in electronic or paper formats.

(5) Log management

The department shall issue a policy that specifies the following:

(a) Who shall maintain the log;

(b) What information shall be captured in the log;

(c) How the log is to be stored; and

(d) How long information kept in the log is to be retained.

Nothing in this rule limits the department from requiring logging in any circumstance that the department deems necessary.

(H) Severability

~~If any paragraph, term or provision of this rule is adjudged invalid for any reason, the judgment shall not affect, impair or invalidate any other paragraph, term or provision of this rule, but the remaining paragraphs, terms and provisions shall be and continue in full force and effect.~~If any portion of this rule or the application thereof to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of the rule or related rules which can be given effect without the invalid portion or application, and to this end the provisions of this rule are severable.