



Ohio Administrative Code

Rule 4775-5-05 Restricting and logging access to confidential personal information in computerized personal information systems.

Effective: January 10, 2011

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

- (A) Access restrictions. Access to confidential personal information that is kept electronically shall require a password or other authentication measure.
- (B) Acquisition of a new computer system. When the board acquires a new computer system that stores, manages or contains confidential personal information, the board shall include a mechanism for recording specific access by employees of the board to confidential personal information in the system.
- (C) Upgrading existing computer systems. When the board modifies an existing computer system that stores, manages or contains confidential personal information, the board 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 board to confidential personal information in the system.
- (D) Logging requirements regarding confidential personal information in existing computer systems.
 - (1) The agency shall require employees of the board who access confidential personal information within computer systems to maintain a log that records that access.
 - (2) Access to confidential information is not required to be entered into the log under the following circumstances:
 - (a) The employee of the board is accessing confidential personal information for official board purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.



- (b) The employee of the board 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.
- (c) The employee of the board 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.
- (d) The employee of the board accesses confidential personal information about an individual based upon a request made under either of the following circumstances:
 - (i) The individual request confidential personal information about himself/herself.
 - (ii) The individual makes a request that the board takes some action on that individuals behalf and accessing the confidential personal information is required in order to consider or process that request.
- (3) For purposes of this paragraph, the board may choose the form or forms of logging, whether in electronic or paper formats.
- (E) Log management. The board shall issue a policy that specifies the following:
 - (1) Who shall maintain the log;
 - (2) What information shall be captured in the log;
 - (3) How the log is to be stored; and
 - (4) How long information kept in the log is to be retained.

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