Ohio Administrative Code

Rule 5122-26-08.1 Security of clinical records systems.

Effective: August 1, 2026

(A) A provider is to have policies and procedures addressing the security of its clinical records system.

(B) If a provider maintains electronic health records (EHRs), the system or module for maintaining the EHRs is to be certified in accordance with Title XXX of the Public Health Service Act (PHSA) and also comply with section 3701.75 of the Revised Code.

A provider is to be able to produce paper and/or electronic copies of client records when a request for such records has been made in accordance with law.

(C) Policies and procedures for providers maintaining an electronically-stored clinical records system are to include consideration of the following components:

(1) Multi-factor authentication - providing assurance regarding the identity of a user and corroboration that the source of data is as claimed;

(2) Authorization - the granting of rights to allow each user to access only the functions, information, and privileges necessitated by their duties;

(3) Integrity - ensuring that information is changed only in a specific and authorized manner. Data, program, system and network integrity are all relevant to consideration of computer and system security;

(4) Audit trails - creating immediately and concurrently with user actions a chronological record of activities occurring in the system;

(5) Disaster recovery - the process for restoring any loss of data in the event of fire, vandalism, disaster, or system failure;

(6) Data storage and transmission - physically locating, maintaining and exchanging data; and

(7) Electronic signatures - a code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual's electronic signature; a computer-generated signature code created for an individual; or an electronic image of an individual's handwritten signature created by using a pen computer. Client record systems utilizing electronic signatures are to comply with section 3701.75 of the Revised Code.

(D) Security of records outside of an EHR - ensuring the security of data stored on personal desktop computers, laptops, portable hard drives, thumb drives, and similar devices by including a constraint that such records are accessible only through multi-factor authentication or are stored in a locked storage unit.

(E) Transfer of EHRs when operations cease - ensuring that if operations cease, EHRs are transferred in accordance with division (A)(15) of section 5119.28 of the Revised Code or, if applicable, 42 C.F.R. 2.19.