Ohio Administrative Code

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

Effective: April 1, 2016

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

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

The provider must be able to produce paper copies of client records upon legally valid requests.

(C) Policies and procedures for providers maintaining a computer-based clinical records system shall include consideration of the following components:

(1) 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 required 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 shall comply with section 3701.75 of the Revised Code.