Ohio Revised Code

Section 3701.75 Authenticating health care records.

Effective: March 22, 1999
Legislation: House Bill 698 - 122nd General Assembly

(A) As used in this section:

(1) "Electronic record" means a record communicated, received, or stored by electronic, magnetic, optical, or similar means for storage in an information system or transmission from one information system to another. "Electronic record" includes a record that is communicated, received, or stored by electronic data interchange, electronic mail, facsimile, telex, or similar methods of communication.

(2) "Electronic signature" means any of the following attached to or associated with an electronic record by an individual to authenticate the record:

(a) 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;

(b) A computer-generated signature code created for an individual;

(c) An electronic image of an individual's handwritten signature created by using a pen computer.

(3) "Health care record" means any document or combination of documents pertaining to a patient's medical history, diagnosis, prognosis, or medical condition that is generated and maintained in the process of the patient's treatment.

(B) All notes, orders, and observations entered into a health care record, including any interpretive reports of diagnostic tests or specific treatments, such as radiologic or electrocardiographic reports, operative reports, reports of pathologic examination of tissue, and similar reports, shall be authenticated by the individual who made or authorized the entry. An entry into a health care record may be authenticated by executing handwritten signatures or handwritten initials directly on the entry. An entry that is an electronic record may be authenticated by an electronic signature if all of the following apply:

(1) The entity responsible for creating and maintaining the health care record adopts a policy that permits the use of electronic signatures on electronic records.

(2) The entity's electronic signature system utilizes either a two-level access control mechanism that assigns a unique identifier to each user or a biometric access control device.

(3) The entity takes steps to safeguard against unauthorized access to the system and forgery of electronic signatures.

(4) The system includes a process to verify that the individual affixing the electronic signature has reviewed the contents of the entry and determined that the entry contains what that individual intended.

(5) The policy adopted by the entity pursuant to division (B)(1) of this section prescribes all of the following:

(a) A procedure by which each user of the system must certify in writing that the user will follow the confidentiality and security policies maintained by the entity for the system;

(b) Penalties for misusing the system;

(c) Training for all users of the system that includes an explanation of the appropriate use of the system and the consequences for not complying with the entity's confidentiality and security policies.