Authenticating Electronic Health Records in RCFs

As licensed Residential Care Facilities ("RCFs") consider converting to electronic health records and increasingly physicians wish to send orders electronically, it is important that RCFs understand what the law requires in this regard, and that they have appropriate policies in place. We have drafted this alert and the policy attached to assist RCFs in this regard.

What is Authentication?

When we refer to "authenticating" electronic health records ("EHR"), we mean the process by which an RCF determines that the record is valid, *i.e.*, that it is what it purports to be, and has not been altered. This is a concern in the electronic world because there is no "original" record, at least as people conceive of an "original" in the paper world.

What is an Electronic Record?

As a starting point, it is important to remember that a "health record" is not just the aggregate file containing the bulk of a person's recorded health information. It is that, but the term is also used to refer to component parts of an overall health record. Thus, a person could ask for a copy of their health record, and mean the entire file that an RCF maintains about the health care that it has provided to them. In the alternative, a person could ask for a copy of a particular page in the file, and this page would also be referred to generically as a health record. It is the same for electronic health records.

Under Ohio law a health record becomes "electronic" if the record is (i) communicated, (ii) received, or (iii) stored by electronic, magnetic, optical, or similar means for storage in an information system or transmission from one information system to another. This would include a record that is communicated, received, or stored by electronic data interchange, electronic mail, facsimile, telex, or similar methods of communication.

What is an Electronic Signature?

An electronic signature is not just what most people think of as a "signature". It is defined in Ohio law as any of the following attached to or associated with an electronic record by an individual to authenticate the record:

1) 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;
2) A computer-generated signature code created for an individual; or
3) An electronic image of an individual's handwritten signature created by using a pen computer.[1]

[1] Note that this last option is becoming increasingly common with physicians.

30100 Chagrin Blvd, Suite 350
Cleveland, OH 44124
216.514.1100
www.RolfLaw.com

Authenticating Electronic Health Records

RCF licensure law provides that an entry that is an electronic record may be authenticated by an electronic signature in accordance with section 3701.75 of the Revised Code ("R.C."). That section provides that all notes, orders, and observations into a health care record shall be authenticated by the individual who made or authorized the entry.

An entry may be authenticated by executing handwritten signatures or handwritten initials directly on the entry. An entry may also 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 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 polices 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.

The sample policy that we drafted tracks the language of R.C. 3701.75 and is for use by those RCFs that are converting, or have converted to, electronic health records, including those that receive physician orders via email. These RCFs should review their electronic health record systems to ensure that they contain all of the above legal requirements.

The law firm of Rolf Goffman Martin Lang Co., LPA provides representation to assisted living providers across the state of Ohio in a wide range of matters, including strategic planning, financing, development, real estate, licensure, tax exemption, policy and admission/residency material development, collections, risk management consultation, and employment counseling and litigation.

ROLF GOFFMAN MARTIN LANG CO., LPA SAMPLE POLICY

Authenticating Electronic Health Records

DEFINITIONS

An *electronic record* is 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, including a record that is communicated, received, or stored by electronic data interchange, electronic mail, facsimile, telex, or similar methods of communication.

An *electronic signature* is defined as any of the following attached to or associated with an electronic record by an individual to authenticate the record:

1) 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;
2) A computer-generated signature code created for an individual;
3) An electronic image of an individual's handwritten signature created by using a pen computer.

POLICY

[RCF Name] utilizes electronic health records. It is the policy of [RCF Name] to authenticate electronic records using electronic signatures in accordance with Ohio law.

PROCEDURE

1. All notes, orders, and observations into a health care record shall be authenticated by the individual who made or authorized the entry.
2. [RCF Name]'s electronic signature system utilizes ***[choose one]*** a two-level access control mechanism that assigns a unique identifier to each user ***[or]*** a biometric access control device.
3. [RCF Name]'s system includes a process monitoring for unauthorized access and forgery of electronic signatures.
4. [RCF Name]'s 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. Prior to being granted access to the electronic records system, each user must complete the following:
    a) Training on use of the system, including confidentiality and security policies and the penalties for not complying with such policies.
    b) Certify in writing that the user will follow the confidentiality and security polices maintained by [RCF Name] for the system.
6. Penalties for misusing the system may include termination of system privileges, and/or termination of employment.