

3364-15-16 Electronic signatures.

(A) Policy statement

Electronic transactions conducted in accordance with this rule shall have the same legal effect as paper-based transactions. The university of Toledo (“UT”) through its information technology (“IT”) security office of information security, which can be found at <http://www.utoledo.edu/it/security/>, shall establish procedures to provide authentication, non-repudiation and integrity to the extent reasonable for each electronic transaction.

(B) Purpose of policy

Prior to using or accepting electronic signatures, Ohio law requires that UT the university establish security procedures that govern the use of electronic signatures and ensure the authenticity, integrity, and non-repudiation of such signatures. The use of electronic signatures, as directed by this rule, can potentially facilitate the timely execution of activities across UT, the university, including personnel actions; contract signatory authorizations; release of educational records (e.g., transcripts, medical degree verifications, third-party credentialing services that request records on behalf of former students (federation credentials verification service, certified screening, etc.)); ~~contract approvals~~; and other activities requiring confirmation of acceptance.

(C) Scope

This policy applies to all electronic transactions entered into on behalf of UT the university.

(D) ~~Definitions~~ Electronic signatures in electronic medical records/electronic health records (“EMRs/EHRs”)

- (1) Electronic signature, an automated function which replaces a handwritten signature with a system generated signature statement, will be utilized for medical records as a means for authentication of transcribed documents, computer generated documents and/or electronic entries. System generated electronic signatures are considered legally binding as a means to identify the author of medical record entries and confirm that the contents are what the author intended.

- (2) Providers will be allowed to utilize electronic signature in accordance with this policy and state and federal regulations regarding such.
- ~~(1) Authenticity—the assurance that the electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.~~
- ~~(2) Domain—a category of persons based on the nature of the identity of the person. For purposes of this policy, electronic transactions may belong to one of the following domains:~~
- ~~(a) Citizen domain~~
- ~~(i) The citizen domain consists of individuals acting on their own behalf or on the behalf of any other individual under a power of attorney.~~
- ~~(ii) The citizen domain includes only those individuals who choose to interact electronically with the state of Ohio.~~
- ~~(iii) The citizen domain also includes state web and application servers that interact with citizens.~~
- ~~(b) Business domain~~
- ~~(i) The business domain consists of corporations, business trusts, partnerships, limited liability companies, associations, joint ventures or any other commercial, charitable or legal entity that interacts electronically with state agencies.~~
- ~~(ii) This domain also includes web and application servers that interact with businesses.~~
- ~~(c) State internal domain~~
- ~~(i) The state internal domain consists of state employees acting on behalf of the state, and any other agent of the state; network components; and web and application servers that use electronic~~

~~transaction-enabled applications to conduct internal state business.~~

~~(ii) The state internal domain also applies to local government representatives for electronic transactions with state government agencies.~~

~~(3) Electronic record — as defined by Chapter 1306 of the Revised Code is a record created, generated, sent, communicated, received, or stored by electronic means.~~

~~(4) Electronic signature — An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.~~

~~(5) Electronic transactions — An action or set of actions, like an exchange of an electronic record and electronic signature between the university and an individual relating to the conduct of such business as:~~

~~(a) Consent to release information;~~

~~(b) Purchase, sell or lease goods, services or construction;~~

~~(c) Transfer funds;~~

~~(d) Facilitate the submission of an electronic record with an electronic signature required or accepted by the UT; or~~

~~(e) Create records formally issued under a signature and upon which the university or any other person will reasonably rely including but not limited to formal communication, letters, notices, directives, policies, guidelines and any other record.~~

~~(6) Integrity — the assurance that the electronic record is not modified from what the signatory adopted.~~

~~(7) Non repudiation — proof that the signatory adopted or assented to the electronic record or electronic transaction.~~

~~(8) Scanned signature — a photocopy, fax, pdf or other copy of a document signed electronically or by hand.~~

~~(9) Security procedure—a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or from detecting changes and errors in a procedure requiring the use of codes or algorithms;—~~

- ~~(a) Identifying words or numbers;~~
- ~~(b) Encryption~~
- ~~(c) Call back or~~
- ~~(d) Other acknowledgement procedures.~~

~~(E) Discipline~~

~~(1) Failure to comply with this policy may lead to disciplinary action up to and including termination.~~

~~(2) The university may repudiate any document signed in violation of its rules, policies, and procedures, and the person signing the instrument may be held personally liable for any obligations incurred.~~

~~(F) Compliance~~

~~— A record, signature or contract may not be denied legal effect or enforceability when it is in electronic form. Electronic form satisfies the law.~~

~~(G) Phone Contacts~~

~~— (1) Office of legal affairs — (419) 530-8411~~

~~— (2) Office of information security — (419) 530-3995~~

~~(GE) Procedure~~

Detailed procedures pertaining to electronic signatures (including definitions of key terms and compliance implications) are contained in a document on the university of Toledo’s institutional compliance webpage.

~~(1) Electronic signatures~~

- ~~(a) — No individual may electronically sign any document for or accept an electronic or scanned signature from another party on behalf of the university except in accordance with this policy.~~

- ~~(b) — Electronic transaction report
 - ~~(i) — Upon request from a unit of the university, the office of information security, in collaboration with the office of legal affairs, shall file an electronic transaction report with the Ohio office of information technology for each set of transactions to be consummated using electronic signatures.~~
 - ~~(ii) — The office of legal affairs shall determine the appropriate domain of each set of transactions.~~
 - ~~(iii) — The office of information security shall conduct a security risk assessment for each set of transactions, identify a security level required for said transactions, and establish security policies and procedures for the transaction set.~~
 - ~~(iv) — The university shall maintain electronic transaction reports for as long as the electronic records of the electronic transaction are retained in accordance with the appropriate record retention schedule.~~~~

- ~~(c) — Facilitating the use of electronic signatures
 - ~~(i) — The university shall, through its normal procurement processes, acquire software to facilitate the use of electronic signatures.~~
 - ~~(ii) — Each person authorized to sign contracts under rule 3364-40-15 of the Administrative Code shall be issued a license for the electronic signature software.~~
 - ~~(iii) — The software shall require the individual to login using his/her “UTAD” credentials in order to electronically sign a document.~~~~

- ~~(d) — The system used to sign electronic contracts shall capture the document at the time of signature and shall securely~~

~~store it so that the signed version may be retrieved in the event of a dispute.~~

~~(e) — Electronic Signature Software~~

~~(i) — The electronic signature software shall require a separate and distinct action for each signature.~~

~~(f) — This policy does not grant contracting authority to any individual or expand the authority already granted in the university document “delegation authority for documents that bind the university.”~~

~~(2) — Scanned Signatures~~

~~(a) — If the office of legal affairs determines that immediate evidence of execution of an instrument is necessary, the university may use and accept scanned signatures.~~

~~(b) — The office of legal affairs shall seek to acquire a hard copy or electronic signature as soon as practicable.~~

(F) References

- (1) Rule 3364-40-15 of the Administrative Code, procurement policy
<https://www.utoledo.edu/policies/administration/finance/pdfs/3364-40-15.pdf>
- (2) Rule 3364-40-08 of the Administrative Code, delegation of signatory authority for documents that bind the university
http://www.utoledo.edu/policies/administration/finance/pdfs/3364_40_08.pdf
- (3) Section 1306 of the Revised Code

Effective: 10/19/2018

CERTIFIED ELECTRONICALLY

Certification

10/09/2018

Date

Promulgated Under: 111.15
Statutory Authority: 3364
Rule Amplifies: 3364
Prior Effective Dates: 03/16/2015