



SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: USE OF ELECTRONIC SIGNATURES, RECORDS, AND DOCUMENTS

PURPOSE

This policy establishes when an electronic signature may replace a written signature and when an electronic record or document may replace a paper record or document and the requirements for electronic signature.

SCOPE

This policy applies to the UAMS workforce and governs all uses of electronic signatures, records, and documents used to conduct official business of the University of Arkansas for Medical Sciences. Such business shall include, but not be limited to, electronic communications, transactions, contracts, Institutional Review Board submissions, grant applications, medical records, and other official documentation.

DEFINITIONS

- A. “Electronic” relates to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- B. A “record” or “document” is information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
- C. An “electronic record” is a record created, generated, sent, communicated, received, or stored by electronic means.
- D. An “electronic document” is a document created, generated, sent, communicated, received, or stored by electronic means.
- E. An “electronic transaction” is a transaction conducted or performed, in whole or in part, by electronic means, records or documents.
- F. An “electronic signature” is an electronic sound, symbol, or process attached to or logically associated with an electronic record or document and executed or adopted by a person with the intent to sign a record or document.
- G. “Public Key” is a cryptographic system that uses two keys. A public key known to everyone and a private key known only to the recipient of the message. When Company A wants to send a secure message to Company B, Company A uses Company B's public key to encrypt the message. Company B then uses its private key to decrypt it. Public and

private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.

- H. A “certificate” is an electronic document used to identify an individual, server, company, or some other entity and to associate that identity with a public key. A certificate provides generally recognized proof of identify for an individual, server, company, or some other entity.
- I. “Certificate Authority”. A Certificate Authority (CA) is a trusted third party whose purpose is to sign certificates for network entities it has authenticated using secure means. Other network entities can check the signature to verify that a CA has authenticated the bearer of a certificate. The certificate authority authenticates the certificate owner's identity and the services that the owner is authorized to use. It also manages the issuance of new certificates and revokes certificates from unauthorized users who are no longer authorized to use them. A certificate authority is considered to be trusted when a user accepts any certificate issued by that certificate authority as proof of the certificate owner's identity.
- J. “Public key infrastructure” (PKI) is a form of information encryption that uses certificates to prevent individuals from impersonating those who are authorized to electronically sign an electronic record or document. A public key is a value provided by some designated authority that, combined with a “private key” derived from the public key, can be used to effectively encrypt messages and digital signatures.
- K. A “private key” is an encryption/decryption key known only to the party or parties that exchange messages. In private key cryptography, a key is shared by the communicators so that each can encrypt and decrypt messages.
- L. “UAMS Workforce” means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

UAMS will accept and use electronic signatures as original signatures in accordance with the Government Paperwork Elimination Act (GPEA) and the Uniform Electronic Transactions Act (UETA). A UAMS electronic record or document with an approved electronic signature is equivalent to a UAMS signed, original record or document.

- A. The UAMS domain is an enterprise certificate authority and the institution trusts certificates issued by its domain.
- B. **Approved electronic signatures.** UAMS Information Technology will establish standards for creating an approved electronic signature. Electronic signatures meet the requirements of an approved electronic signature under this policy when the user has signature authority for UAMS and the electronic signature is
 - a. unique to the person using it,

- b. capable of verification,
 - c. under the sole control of the person using it, and
 - d. linked to data in such a manner that the data cannot be altered after signature. If the data is somehow altered after signature, the signature is invalidated.
- C. Signature required by UAMS policy
- a. Where UAMS policy requires that a record have the signature of a responsible person, that requirement is met when the electronic record has associated with it an electronic signature using an approved electronic signature method in accordance with standards established by UAMS Information Technology.
 - b. Where UAMS policy requires that a written document have the signature of a responsible person, that requirement is met when the electronic document has associated with it an electronic signature using an approved electronic signature method in accordance with standards established by UAMS Information Technology.
- D. Signature required by law
- a. Where there is a legal requirement beyond UAMS policy that a record have the signature of a responsible person, that signature requirement is met when the electronic record has associated with it an electronic signature using an approved electronic signature method.
 - b. Where there is a legal requirement beyond UAMS policy for a written document, that requirement is met when an electronic document has associated with it an electronic signature using an approved electronic signature method
- E. Contracts
- a. Where both UAMS and the other party to a contract have agreed to conduct a transaction by electronic means, a contract may be signed using an approved electronic signature method. Either party to an agreement has the right to refuse to conduct a transaction by electronic means.
 - b. If both parties have agreed to conduct business by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.
 - c. If a party requests an original, signed paper document, a UAMS electronic document with an electronic signature will either be 1) sent electronically or 2)

printed and the printed paper document, which is equivalent to an original signed paper document, will be sent to the requesting party.

F. Unauthorized electronic signatures

- a. The unauthorized use of another user's electronic signature will result in disciplinary action in accordance with UAMS Policy 4.4.02.

PROCEDURE

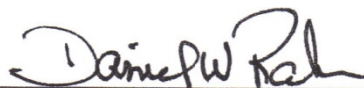
Acceptable UAMS electronic signature mechanisms:

- A. Digital Signature: a digital signature is a cryptographic signature (a digital key) that authenticates the user, provides non-repudiation, and ensures message integrity. This is the strongest signature type and is the preferred mechanism.
- B. Button, PIN, Biometric, or Token: a frequently used e-signature methodology includes clicking a button or entering a unique personal identification number (PIN), electronic identification, token, or biometric scan at the completion of an entry for the signature process. Any such mechanism for e-signature must meet the requirements of this policy in order to be acceptable, including being under the sole control of the person using it, capable of verification, and linked to the data in such a manner the data cannot be altered after signature.
- C. Any other e-signature mechanism must be pre-approved by IT Security prior to use.

Related Policies:

5.3.01 Professional/Consultation and Commodity/Services Contracts

3.1.15 Confidentiality policy

Signature:  _____

Date: May 11, 2011